

Research Report

C00259285 – Nathan Murphy

Contents

Introduction.....	2
Type of Tools	2
Wireshark.....	2
TCPdump	3
Python	3
Visual Studio Code	4
Flask.....	4
Pyshark.....	5
Tshark.....	6
Summary	6
References.....	7

Introduction

What is Network analysis? This is the constant monitoring of traffic going in and out of a network. A network analysis tool is used to detect any anomalies going in and out of a network. This research document is going to be used as an aid to build a Simplified Network Analysis Tool. The goal is to build a fully functioning Network analysis tool for students of IT. This tool will should be used so students can easily understand how a network analysis tool works and what are the signs they should look for when monitoring a network. This document will consist of other tools as a comparison, software that will be used, any libraries etc that will need to be used.

Type of Tools

Wireshark

Wireshark is the world's foremost network protocol analyser. It has the ability to see what is happening on a network at a microscopic level. It is the standard across many industries and educational institutions.

Wireshark has many features some of them are:

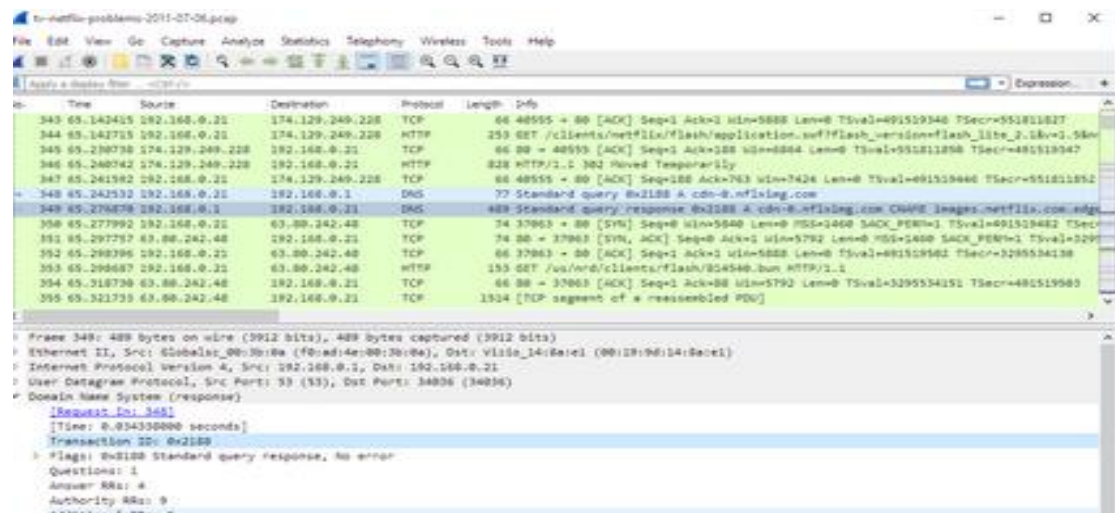
- Live capture and offline analysis
- Multi-platform
- Decryption support for many protocols
- Captured network data can be browsed via GUI

The main purpose of Wireshark is so Network administrators can troubleshoot any network problems and so Network security engineers use it to examine security problems.

Although Wireshark has many features there is a few that it does not provide which may be useful:

- Wireshark does not provide an intrusion detection system. What does this mean? Wireshark will not produce a warning when there is suspicious activity on the network. But it might help figure out what is happening.
- “Wireshark will not manipulate things on the network, it will only “measure” things from it. Wireshark doesn't send packets on the network or do other active things (except domain name resolution, but that can be disabled).”

Resources that Wireshark needs depend on the environment the user is on and the size of the capture file that is being analysed. If Wireshark runs out of memory it will crash. ([Wireshark Foundation, About](#))



TCPdump

TCPdump is a packet sniffer. It has the ability to capture traffic that passes through a machine. It operates on a packet level, what does this mean? It is able to capture actual packets that are going in and out of a machine. TCPdump can either save the whole packet or only the headers.

TCPdump understands protocols and host names this means it will try to see the host that sent each packet and provide a name instead of an ip address.

Filters can be applied if a packet matches the filter tcpdump will acknowledge the packet and will wither saves it to a file or dumps it on a screen. Otherwise, the packet will be ignored.

A negative about tcpdump in general it doesn't give you too much information about packets. It can't understand different protocols. Tcpdump is a command line tool so the ability to present info is limited. ([Alexander Sandler, System Administrator Articles](#))

Python

“Python is an interpreted, interactive, object-oriented programming language. It incorporates modules, exceptions, dynamic typing, very high-level dynamic data types, and classes. It supports multiple programming paradigms beyond object-oriented programming, such as procedural and functional programming. Python combines remarkable power with very clear syntax. It has interfaces to many systems calls and libraries, as well as to various window systems, and is extensible in C or C++. It is also usable as an extension language for applications that need a programmable interface. Finally, Python is portable: it runs on many Unix variants including Linux and macOS, and on Windows.”

“Python is a high-level general-purpose programming language that can be applied to many different classes of problems.

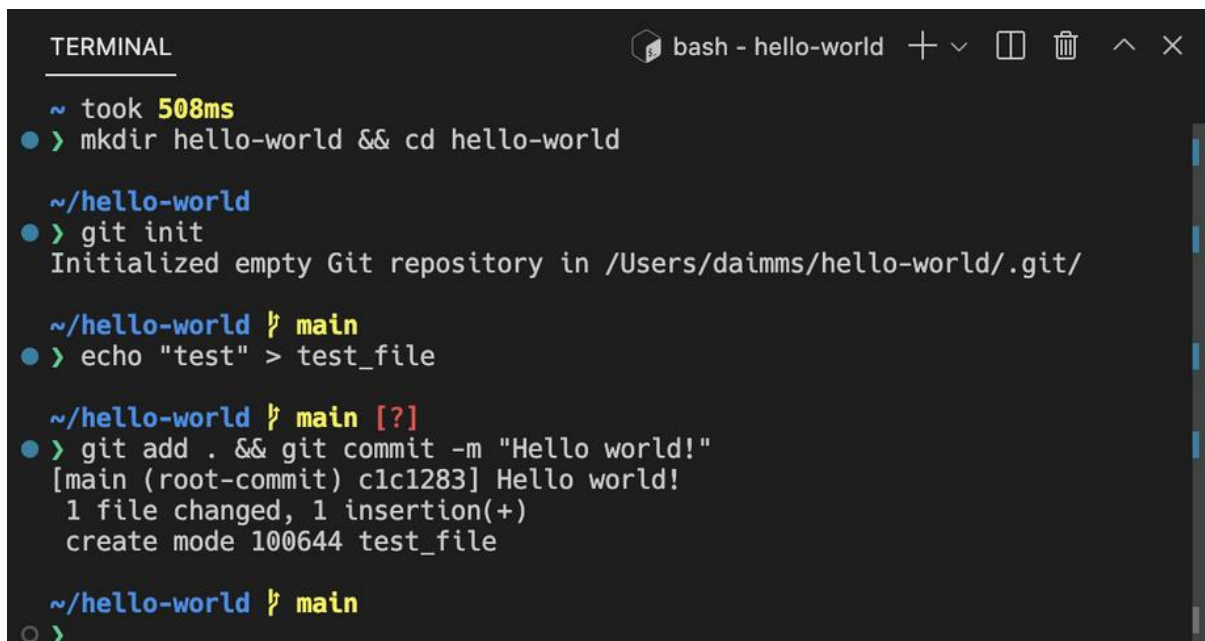
The language comes with a large standard library that covers areas such as string processing (regular expressions, Unicode, calculating differences between files), internet protocols (HTTP, FTP, SMTP, XML-RPC, POP, IMAP), software engineering (unit testing, logging, profiling,

parsing Python code), and operating system interfaces (system calls, filesystems, TCP/IP sockets) ([Python Software Foundation, General Python FAQ](#))

Visual Studio Code

“Visual Studio Code, commonly referred to as VS Code, is an integrated development environment developed by Microsoft for Windows, Linux, macOS and web browsers. Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded version control with Git. Users can change the theme, keyboard shortcuts, preferences, and install extensions that add functionality.”

VSCoDe has an integrated terminal that starts at the root. The integrated terminal can run commands just like a standalone terminal. VSCoDe can support almost every major programming language (Python, C, C++) ([Visual Studio Code, Docs](#))



```
TERMINAL
bash - hello-world + - [ ] [ ] ^ x

~ took 508ms
● > mkdir hello-world && cd hello-world

~/hello-world
● > git init
Initialized empty Git repository in /Users/daimms/hello-world/.git/

~/hello-world ♯ main
● > echo "test" > test_file

~/hello-world ♯ main [?]
● > git add . && git commit -m "Hello world!"
[main (root-commit) c1c1283] Hello world!
1 file changed, 1 insertion(+)
create mode 100644 test_file

~/hello-world ♯ main
○ >
```

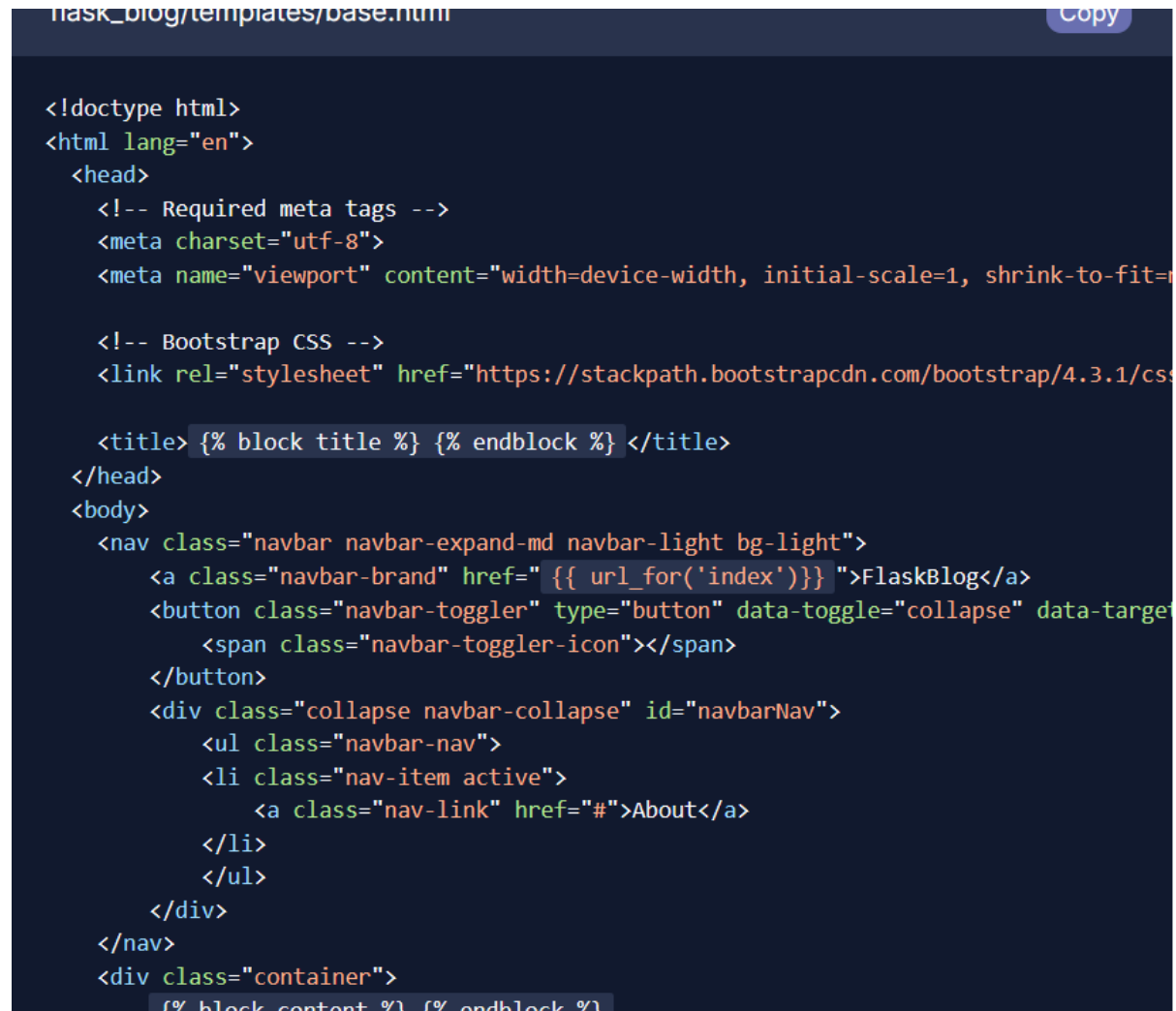
Flask

“Flask is a small and lightweight Python web framework that provides useful tools and features that make creating web applications in Python easier. It gives developers flexibility and is a more accessible framework for new developers since you can build a web application quickly using only a single Python file. Flask is also extensible and doesn’t force a particular directory structure or require complicated boilerplate code before getting started.” ([Flask, Flask Documentation](#))

Flask uses Jinja template engine to dynamically build HTML pages it uses familiar Python concepts such as variables, loops and lists. ([Digital Ocean, Tutorial](#))

“Jinja is a fast, expressive, extensible templating engine. Special placeholders in the template allow writing code similar to Python syntax. Then the template is passed data to render the final document.” ([Jinja, Jinja Documentation](#))

To use Flask, you will need a Python 3 programming environment.



```
flask_blog/templates/base.html Copy

<!doctype html>
<html lang="en">
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css">

    <title> {% block title %} {% endblock %} </title>
  </head>
  <body>
    <nav class="navbar navbar-expand-md navbar-light bg-light">
      <a class="navbar-brand" href="{{ url_for('index') }}">FlaskBlog</a>
      <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarNav">
        <span class="navbar-toggler-icon"></span>
      </button>
      <div class="collapse navbar-collapse" id="navbarNav">
        <ul class="navbar-nav">
          <li class="nav-item active">
            <a class="nav-link" href="#">About</a>
          </li>
        </ul>
      </div>
    </nav>
    <div class="container">
      {% block content %} {% endblock %}
    </div>
  </body>
</html>
```

Pyshark

“PyShark is a Python utility and library designed to parse packets using Wireshark dissectors. Unlike some other packet parsing modules, PyShark doesn’t directly parse packets; instead, it leverages tshark’s ability to export XMLs and uses them for parsing. This approach allows PyShark to use all installed Wireshark dissectors, making it a versatile choice for network analysis.” ([Stefen Selvidge, Pyshark](#))

Pyshark is a Python wrapper for tshark.

Tshark

“TShark is a network protocol analyser. It lets you capture packet data from a live network, or read packets from a previously saved capture file, either printing a decoded form of those packets to the standard output or writing the packets to a file. TShark's native capture file format is pcap format, which is also the format used by Wireshark and various other tools.” ([Wireshark, tshark manual page](#))

Tshark works just like tcpdump. It uses pcap library to capture the network traffic from the first available interface and then a summary will be displayed.

Key features of Tshark are:

- Packet Capture – Tshark captures traffic flowing in a network from different interfaces.
- Filtering – Tshark supports display filters and capture filters
- Protocols – Tshark has the capability of interpreting multiple network protocols
- Command-line Interface – Tshark operates through a command line
- Export and Analysis – Tshark is able to export captured data through various methods (e.g. plain text, XML, JSON)

Advantages of Tshark:

- Tshark has flexible filtering as it supports both capture and display filters
- Due to Tshark using a command line this means it uses fewer resources
- Tshark has the ability to be automated
- Multiple options for exporting data

Summary

The document will be used as an aid for building a Simplified Network Analysis Tool which is targeted at students of IT to gain a better understanding of how a Network Analysis tool is used and what to expect as an outcome with a simple point and click interface. This document has gone through tools that are currently being used to gain insight into their advantages and disadvantages so it can be implemented to my own tool. It has information on software's and libraries I expect to use during the build of this tool.

References

Wireshark Foundation, About, Available at <https://www.wireshark.org/about.html> (Assessed: 2nd December 2024)

Wireshark, Introduction, Available at https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html (Assessed 10th February 2025)

Justin Sheli, Blog, Available at <https://www.electric.ai/blog/why-you-need-to-deploy-network-monitoring> (Assessed: 2nd December 2024)

Alexander Sandler, System Administrator Articles, Available at <http://www.alexonlinux.com/tcpdump-for-dummies> (Assessed: 3rd December 2024)

Python Software Foundation, General Python FAQ, Available at <https://docs.python.org/3/faq/general.html#what-is-python> (Assessed: 3rd December 2024)

Flask, Flask Documentation, Available at <https://flask.palletsprojects.com/en/stable/> (Assessed: 5th December)

Wireshark, tshark Manual Page, Available at <https://www.wireshark.org/docs/man-pages/tshark.html> (Assessed 10th December)

Stefen Selvidge, Pyshark, Available at <https://celeryq.org/pyshark/> (Assessed 10th December)

Digital Ocean, Tutorial, Available at <https://www.digitalocean.com/community/tutorials/how-to-make-a-web-application-using-flask-in-python-3> (Assessed 18th February 2025)

Jinja, Jinja Documentation, Available at <https://jinja.palletsprojects.com/en/stable/> (Assessed 19th February 2025)

Visual Studio Code, Docs, Available at <https://code.visualstudio.com/docs/terminal/basics> (Assessed 19th February 2025)