

Identifying Security threats

Cyber Security



Noel Rottebiller N0931129

Maks Miketa N0945100

Jawad Naeem N0972124

Phillip Radasevic N0930646

Contents

[What are PCAP Files? 2](#_Toc94552660)

[PCAP File Global Header Analysis 2](#_Toc94552661)

[The length of the global header 2](#_Toc94552662)

[The magic number and the endianness of the PCAP file 2](#_Toc94552663)

[The major and minor version numbers of the file format 2](#_Toc94552664)

[The SnapLength 2](#_Toc94552665)

[The data link type 2](#_Toc94552666)

[Analysis of DHCP frame 2](#_Toc94552667)

[The timestamp indicating when this packet was captured 2](#_Toc94552668)

[The actual GMT time corresponding to this timestamp 2](#_Toc94552669)

[The length of this DHCP frame 2](#_Toc94552670)

[The source and destination MAC addresses of the captured communication 2](#_Toc94552671)

[The source and destination IP addresses of the captured communication 2](#_Toc94552672)

[The name of the host PC 2](#_Toc94552673)

[Using Regular Expression to find susceptible website 2](#_Toc94552674)

[Finding search engine of the website 2](#_Toc94552675)

[Generic Python code to identify more potential security threats 3](#_Toc94552676)

[Bibliography 3](#_Toc94552677)

# What are PCAP Files?

# PCAP File Global Header Analysis

## The length of the global header

A PCAP file begins with the global header which has a fixed size of 24 bytes consisting of the magic number which are the first 4 bytes of the file. The next 2 bytes of the file are the major version number followed by next 2 bytes that are the minor version number of the file. The next 4 bytes represent the correction time in seconds between GMT and the local timezone of the packet header timestaps. The next 4 bytes show the accuracy of the timestamp in the capture. The next 4 bytes show the snaplength and the last 4 bytes show the data link type resulting in 24 bytes within the global header.

## The magic number and the endianness of the PCAP file

The magic number is 32 bits long and is used to detect the file format itself and the byte ordering. The magic number determines if the file is a big or little-endian file. Endianness is the ordering of bytes where little-endian stores the least significant bytes before the more significant bytes and big-endian stores the most significant bytes before the less significant bytes. If the magic number has the value of 0xa1b2c3d4, the file is big endian. If the hexadecimal value is 0xd4c3b2a1, file is little endian and must be processed in reverse order. The magic number of the PCAP file is 0xd4c3b2a1 therefore, it is a little-endian file.

## The major and minor version numbers of the file format

The major and minor versions are unsigned values that give the number of the current major/minor version of the file format. The major version of the file format is 2 and the minor version is shown as 4 so the version of the file is 2.4.

## The SnapLength

The snaplength is the snapshot length for the capture. A captured packet in the file may not contain all data in the packet as appeared on the network so the captured file might contain at most the first N bytes of each packet for some value of N. The value of N is the snapshot length which in this file is 65535.

## The data link type

The data link type specifies the link layer type value which is 1 in the captured file. Number 1 value means that the data link type used is ethernet.

# Analysis of DHCP frame

## The timestamp indicating when this packet was captured

## The actual GMT time corresponding to this timestamp

## The length of this DHCP frame

## The source and destination MAC addresses of the captured communication

## The source and destination IP addresses of the captured communication

## The name of the host PC

# Using Regular Expression to find susceptible website

# Finding search engine of the website

# Generic Python code to identify more potential security threats

# Bibliography