IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁘ Impact Factor 8.102 ⁘ Peer-reviewed / Refereed journal ⁘ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12606

Crafting IPv4 Packets using Scapy to Implement Network Steganography

Prof. Dr. Shraddha Khonde[1], Rutuja Gaikwad[2], Pratiksha Chavan[3],

Dnyaneshwari Rakshe[4]

Students, Department of Computer Engineering, MES College of Engineering, Pune [1,2,3,4]

Abstract: A technique used for hidden communication between two covert parties. It is an art of hidden communication. It also relates to the areas like network protocols and security for practical data hiding in communication networks using Transmission Control Protocol/Internet Protocol (TCP/IP). Network steganography uses communication protocols such as TCP/IP. Such methods make it harder to detect and eliminate. In a typical steganography using network the modification of a single network protocol occurs. Such modification can be to the Protocol Data Unit. Network steganography shelters a broad spectrum of techniques.

Keywords: Network Protocols, Covert Communication, Storage-based Covert Channel, System Security, Network Security, Steganography, Encryption, TCP/IP, IPv4, Scapy

INTRODUCTION

As every organisation, every person wants to keep information and communication secrete and safe. Steganography is the method to hide data inside cover, that person even cannot detect that this cover or media contain a covert message. Image, audio and video are media to insert a secrete message inside it. But, why not to use the already existing media or a cover to hide a message, here, is technique to hide a message inside a cover which can be the network protocols.

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Network protocols are the reason you can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

To save the extra storage use, we can hide the message inside the network protocol, in its various fields such as option field and identification field. It can be implemented by creating covert channels inside a option field of IP protocol header.

1. IP Protocol

In computer networking internet protocol is a medium or set of rules for routing and addressing packets of particular data for communicating over the internet through packets. Packet is nothing but small pieces of data that going to traverse. The structure of IP packet consists of IP header attached to each packet.

1.1 IP Header

IP header contains all the information like, source IP address, destination IP address, flag, length. It consists of two parts a fix part and a variable part. The fields in the IP header are as follows

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁐ Impact Factor 8.102 ⁐ Peer-reviewed / Refereed journal ⁐ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12606

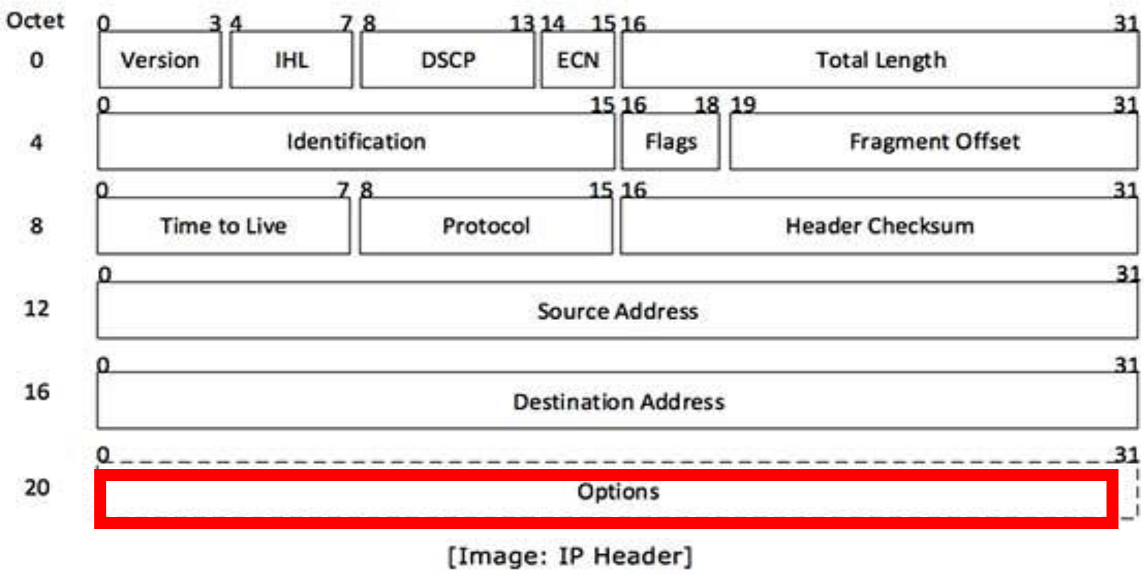

Figure 1:IP Header

1.2 IP Options

As the name implies, it is not mandatory to use. Hence, this space can be utilized to communicate covertly by inserting a secrete message in this field

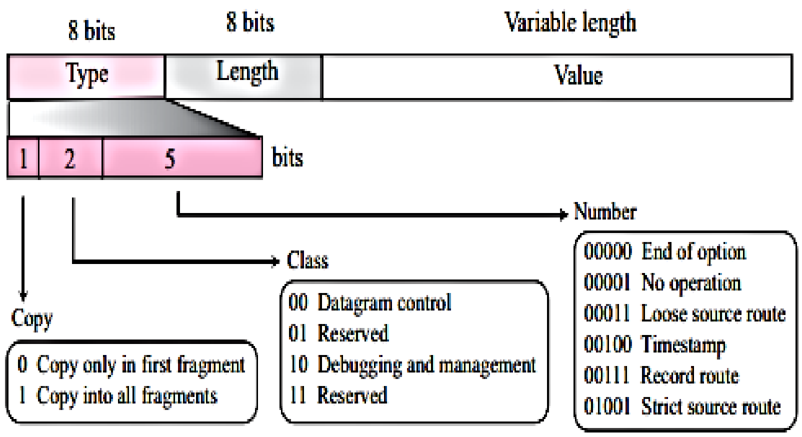

Figure 2:IP Option Field Structure

IP Option consists of Type field which is 8 bits long having 3 subfields

- Copy
- Class
- Number

1.2 Timestamp Option

```
0           7           15          23          31
+-----------+-----------+-----------+-----------+
|   type    |  length   |  offset   |overflow| flags |
+-----------+-----------+-----------+-----------+
|                internet ID                    |
+-----------+-----------+-----------+-----------+
|                time stamp                     |
+-----------+-----------+-----------+-----------+
```

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁑ Impact Factor 8.102 ⁑ Peer-reviewed / Refereed journal ⁑ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12606

In the timestamp, option type is 68 decimals (i.e., option class = 2 and option number = 4),
option length is the number of octets with a maximum of 4, timestamp = a right-justified, 32-bit timestamp. In this project we are using timestamp.

LITERATURE SURVEY

Network steganography is recent steganography technique, while image, audio and video steganography has been favourite topic of researchers. In this section, we have look on previous work and research related to network and protocol steganography.

As per our knowledge based on research, Network steganography has not been that much researched topic. Rowland in [12] suggested the use of IP identification field which is normally used for identifying the fragments of an IPv4 packet. Many other approaches [4][7][8] proposed steganographic method to hide secret message into the identification field of IP packet header. In [4] Punam Bedia, Arti Duab have proposed a network steganography using the overflow field of timestamp option in an IPv4 packet. In [13] stated that, the packet timings are varied in order to create covert channel.

These channels are more complex than storage type covert channel. Wireshark application (Wireshark is a freely available packet analyser tool) [9] at the receiving end. The warning messages are automatically highlighted by Wireshark in yellow. Moreover, if more covert messages like these are sent over the network, the generation of a large number of warning indications can draw the attention of a network administrator about some suspicious communication.

Experimental Setup –

On the LINUX environment, communication setup is between two LAN connected nodes. One is sender and another is receiver. Using the IP address of the receiver, sender sends the covert channel thorough the protocol which is IP protocol.

This implementation method uses **Scapy** which is the Python's networking library used for the network packet manipulation. Using scapy the covert data is added in the timestamp field of timestamp option. While traversing the covert message,

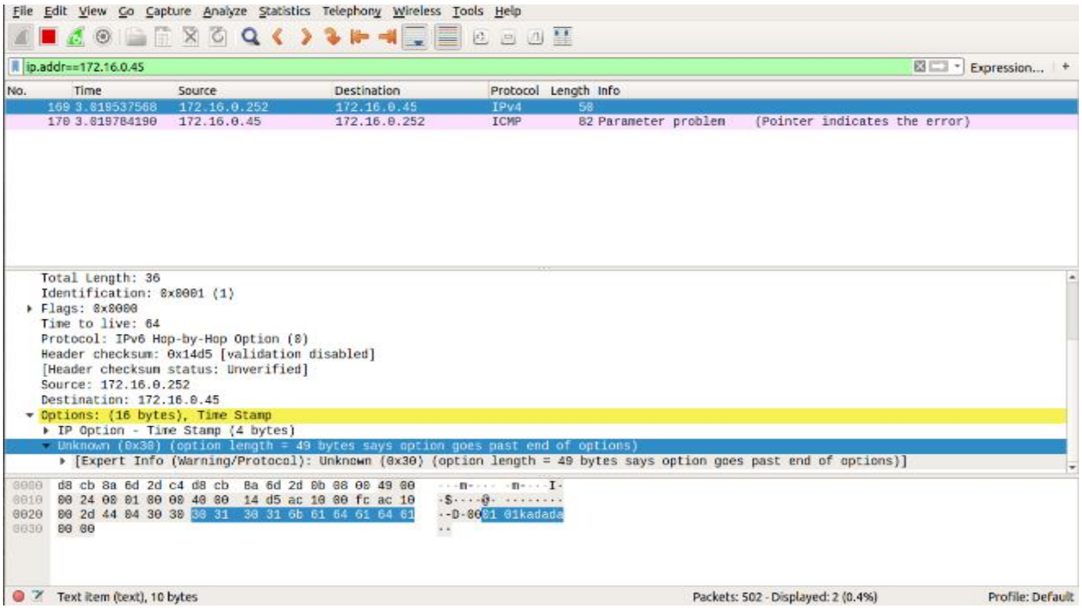

Figure 3:Warning Message by Wireshark (Yellow)

Wireshark (Packet-sniffer) a network protocol analysis application which captures packet from a network connection can identify the unusual patterns or packet content in the traffic like malformed packet. The image Fig.4 shows the warnings showed by the Wireshark while traversing the packet. It is due to overfitting of the packet.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁙ Impact Factor 8.102 ⁙ Peer-reviewed / Refereed journal ⁙ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12606

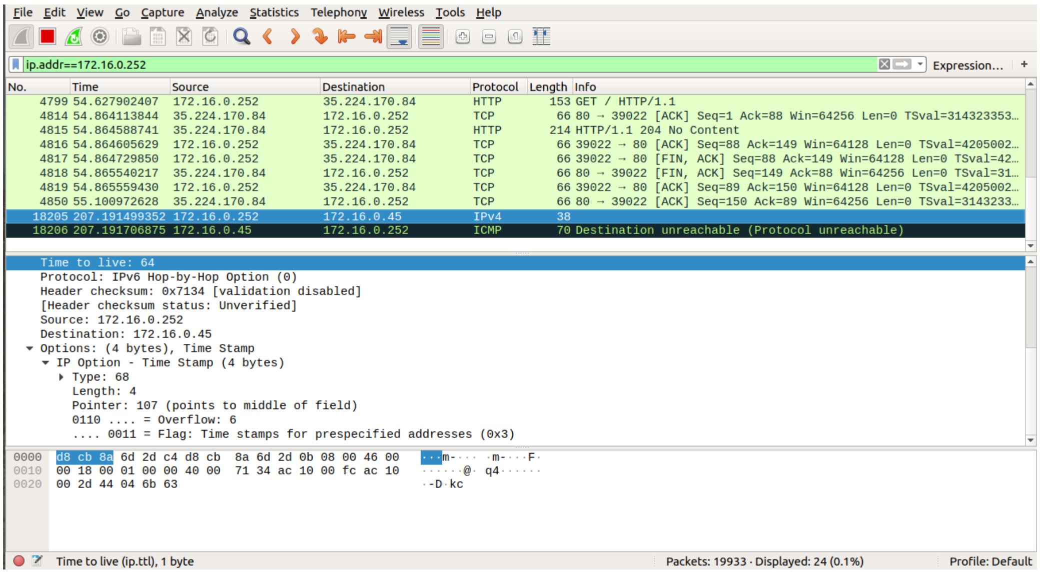

Figure 4:At sender's side

Here through the sender's node the text data in the byte form is transferred to the receiver while the receiver can track that data through the Wireshark or Scapy sniffer. The covert data is hidden from the other ordinary user of the Wireshark.

Fig 5 shows the data that is captured by the receiver after successfully traversing the covert message.

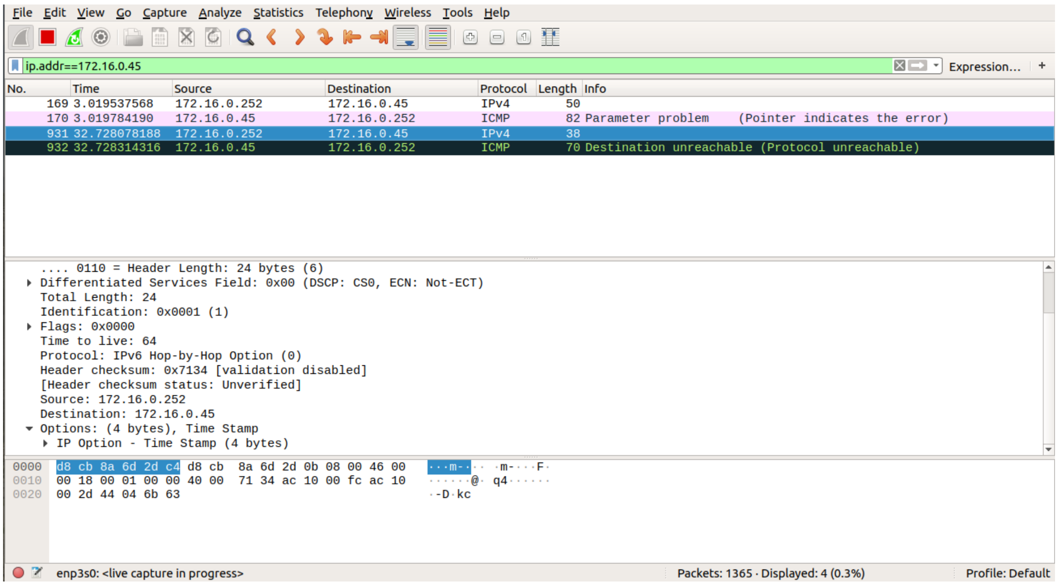

Figure 5:At receiver's side

CONCLUSION

This method of network steganography uses timestamp option field instead of other like identification field and using a text data to be traversed avoiding extra efforts to decrypt the data from the bits to text. Without getting caught in the Wireshark the covert data is traversed through the setup system in the view of string. This is the way by which text data is traversed.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁙ Impact Factor 8.102 ⁙ Peer-reviewed / Refereed journal ⁙ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12606

REFERENCES

[1] Avish Dhamade, Krunal Panchal Computer Science Engineering Department, L. J. Institute of Engineering Technology, Gujarat Technological University 2019.

[2] Namrata Singh Dept. of CSE ABES Engg. College Ghaziabad, India, Jayati Bhardwaj Dept. of CSE ABES Engg. College Ghaziabad, India, Gunjan Raghav Dept. of CSE ABES Engg. College Ghaziabad, India 2020.

[3] K. Szczypiorski, HICCUPS: Hidden Communication System for Corrupted Networks, In Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, pp. 31-40, October 22-24, 2003.

[4] Punam Bedia, Arti Duaba, Department of Computer Science, University of Delhi, Delhi 110007, India 2020.

[5] B. Jankowski, W. Mazurczyk, K. Szczypiorski, Information Hiding Using Improper Frame Padding - 14th International Telecommunications Network Strategy and Planning Symposium (Networks), 2010.

[6] Amritha Sekhar 1, Manoj Kumar G.2, Prof. (Dr.) M. Abdul Rahiman3 Student, Department of CSE, LBS Institute of Technology for Women, Thiruvananthapuram.

[7] W. Fraczek, W. Mazurczyk, K. Szczypiorski, Stream Control Transmission Protocol Steganography, Second International Workshop on Network Steganography (IWNS 2010) co-located with the 2010 International Conference on Multimedia Information Networking and Security (MINES 2010), November 2010.

[8] Amritha Sekhar 1, Manoj Kumar G.2, Prof. (Dr.) M. Abdul Rahiman3 Student, a. Department of CSE, LBS Institute of Technology for Women, b. Thiruvananthapuram, India

[9] Hamza Khaddar*, Merouane Bouzid** *(Department of Telecommunication, LCPTS Lab USTHB University, Algeria) ** (Department of Telecommunication, LCPTS Lab USTHB University, Algeria)

[10] C. G. Girling, Covert Channels in LAN 's. USA, IEEE Transactions on Software Engineering, 1987 [18] Deepa Kundur and Kamran Ahsan. "Practical Internet Steganography: Data Hiding in IP", In Proceedings of Texas Workshop on Security of Information Systems, April 2003.

[11] Hamza Kheddar, Merouane Bouzid, Department of Telecommunication, LCPTS Lab USTHB University, Algeria, "Implementation of Covert Channel Method Based on IPv4 Identification Field over NS-3, March 2015.

[12] Rowland, Craig H. (1997) "Covert channels in the TCP/IP protocol suite" First Monday, 2(5)

[13] Namrata Singh, Jayati Bhardwaj, Gunjan Raghav, Dept. of CSE ABES Engg. College Ghaziabad, India International Journal of Computer Applications (0975 – 8887) Volume 174 – No.2, September 2017

[14] Wireshark-Go Deep, https://www.wireshark.org, (2019, accessed 19 Sept 2019).

