

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/316733045>

Packet tracing and analysis of network cameras with Wireshark

Conference Paper · April 2017

DOI: 10.1109/ISDFS.2017.7916510

CITATIONS

21

READS

2,594

2 authors, including:



[Resul Das](#)

Firat University

113 PUBLICATIONS 2,481 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Heart disease [View project](#)

Packet Tracing and Analysis of Network Cameras with Wireshark

Resul Das

Department of Software Engineering, Firat University, 23119, Elazig, Turkey
rdas@firat.edu.tr

Gurkan Tuna

Department of Computer Programming, Trakya University, 22020, Edirne, Turkey
gurkantuna@trakya.edu.tr

Abstract—People think that their identity on the internet is different from their real identity and that they do not do with their own identities. On the other hand, the confidentiality and protection of personal information on unreliable networks such as the internet is an important question. In this study, a sample application on network packet tracing and analysis of network cameras with wireshark program is realized to show how partial access to personal information and location information is obtained.

Keywords—Location Detection, Wireshark, OSI Reference Model Layers, Network Based Chat Systems

I. INTRODUCTION

In the past, the most common way to connect computers between multiple offices was to use a leased line. Basically, leased lines are private network connections that a telecommunications company can lease to its customers. Leased lines allowed companies to form Wide Area Networks (WANs) and this way extended their private networks beyond the near-geographical areas. Although leased lines were secure, their costs were high and depended on the distance between offices. However, different from the past, today, the Internet is more accessible than ever and Internet service providers (ISPs) continue to offer faster, more reliable services at lower cost than leased lines. To take advantage of this, many businesses have replaced leased lines with new technologies that use Internet connections without sacrificing performance. To provide security for Internet users in computer networks, one of the early solutions was the use of proxy servers which provide services to their clients. However, later on proxy servers were replaced with firewalls in spite of the fact that web proxies are still in use since they facilitate access to content on the World Wide Web (WWW) while providing anonymity [1]. On the other hand, to connect remote offices to a central office securely, Virtual Private Networks (VPNs) are formed [2].

In the last decade, businesses have started by setting up intranets, which are private internal networks designed exclusively for use by company employees [3]. Intranets have enabled remote colleagues to work with technology such as desktop sharing. By adding a VPN, an enterprise can extend all intranet resources to employees working from remote offices or homes. But VPN is a structure that can be used to provide privacy and accessibility at a personal level, apart from business and other data transmission between remote networks [4].

In computer networks, although User Datagram Protocol (UDP), working on 4th layer of Open Systems Interconnect (OSI) reference model, is preferred in real-time data transmissions such as voice and video transmission over WANs and chat applications, it lacks some security features that are supported by Transmission Control Protocol (TCP) [5]. UDP, how it works is shown in Fig. 1, reduces the data transmission time by not performing connection establishment, flow control and retransmission mechanisms and this way increases the speed of the data transfer [6].

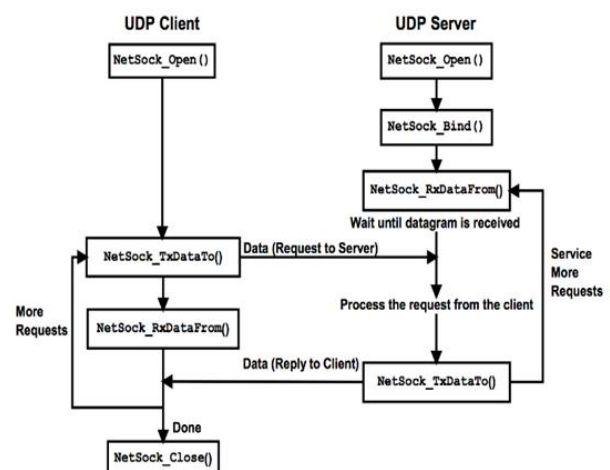


Fig. 1. How UDP packets are delivered [6]

When data transmission over public networks is realized, capturing network communication packets can be used to reveal a lot of information such as the devices used by the senders, the location they are in [7]. However, the accuracy of the information is variable and depends on how the packet analysis is done and the third party software that the sender/receiver uses for communications. Hence, there is a need to measure the accuracy of information revealed through the packet analysis. In this study, the usability and reliability of Wireshark for packet tracing and analysis is investigated. The remainder of the paper is as follows. Theoretical information on software based audio and video transmission systems is given in Section 2. Data confidentiality on the Internet and software based tools for packet tracing and analysis is explained in Section 3. A case study is given in this section. Finally Section 4 concludes the paper.

II. BACKGROUND ON SOFTWARE BASED AUDIO AND VIDEO TRANSMISSION SYSTEMS

Session Traversal Utilities for Network Address Translation (NAT) (STUN) is a protocol serving as a tool for other protocols in dealing with NAT traversal and can be used by an endpoint to determine the Internet Protocol (IP) address and port allocated to it by the NAT [8]. Also, it can be used to check connectivity between two endpoints, and as a keep-alive protocol to maintain NAT bindings. Typically, STUN is a tool used by other protocols such as Interactive Connectivity Establishment (ICE), Session Initiation Protocol (SIP), or WebRTC [8, 9]. SIP is a protocol developed for providing telephone service over the Internet. SIP is used for call setup between two or more users on an IP network, changing session related parameters during the call, and finally resolving and terminating the call [10, 11]. Host computers provide a means for discovering the presence of a network address translator and for discovering the mapped Internet Protocol (IP) address and port number that NAT service allocates for NAT for UDP connections to remote computers [12]. The protocol is usually from a public third party network server (STUN server) located on the other side of the NAT (public).

During a conversation between two users using Voice over Internet Protocol (VoIP), the voice is picked up and compressed using certain codecs [13]. The voice of both parties is compressed using the same codec and sent to each other via the Internet. Other than SIP, technologies such as H323, MGCP and SS7, which are popular in VoIP service providers' infrastructure, are used [14]. In VOIP applications, algorithms such as G.729, G.723, G.726 and G.711 are used for voice compression [15-17]. G.711 is the basic decoder of the Public Switched Telephone Network (PSTN). Mostly, G.729 codecs are used even though G.723 is the best one in terms of compression; however the Mean Opinion Score (MOS) of G.723 is less than the others [15-17].

Given the bandwidth used, the G.729A offers impressive sound quality [18]. This is done by using the Adjoint Structure Algebraic Code Stimulated Linear Estimation (CS-ACELP) [19]. However, due to the patents, G.729A cannot be used without paying a license fee [18]. However, it is extremely popular and therefore supported by many different phones and systems.

The Skype protocol is a proprietary Internet telephony network based on the Peer-to-Peer architecture used by Skype, an application that provides video chat and voice call services over its peer-to-peer IP telephony network [20]. The features of the protocol are not covered by Skype and the official applications using the protocol are being developed in closed source. The Skype network does not work with many of the other VoIP networks without an appropriate license from Skype. There have been many attempts in the past to investigate and / or reverse engineer the protocol to expose the protocol, investigate security, or allow unofficial customers [21]. The Skype network includes three types of entities: super nodes, ordinary nodes and login server. Each client maintains a host cache with the IP address and port numbers of the accessible supernodes. The Skype user directory is distributed between non-centralized and networked supernodes [22]. Skype user names are unique. The entries must provide a username and password or other authentication information. Whenever they come together, each caller provides identification and privilege documents to the other. Everyone confirms the other's key before the session is allowed to carry the messages. Forwarded messages are encrypted; hence, no intermediary node has access to the content of these messages.

When a Skype client is run, the client authenticates the user with the sign-in server, announces its presence to other partners, identifies the NAT and firewall behind it, and discovers nodes with common IP addresses. To connect to the Skype network, a valid entry in the host cache must exist. As shown in Fig. 2, a TCP connection must be established, otherwise the login will fail.

```

1. start
2. send UDP packet(s) to HC
3. if no response within 5 seconds then
4.   attempt TCP connection with HC
5.   if not connected then
6.     attempt TCP connection with HC on port 80 (HTTP)
7.     if not connected then
8.       attempt TCP connection with HC on port 443 (HTTPS)
9.       if not connected then
10.        attempts++
11.        if attempts == 5 then
12.          fail
13.        else
14.          wait 6 seconds
15.          goto step 2
16. Success

```

Fig. 2. How Skype basically works [20]

III. DATA CONFIDENTIALITY ON THE INTERNET AND SOFTWARE BASED TOOLS FOR PACKET TRACING AND ANALYSIS

It is possible to access IP cameras if simple usernames and passwords are set or not set at all. Also, those cameras can be traced to find out personal information of their owners. Because, the confidentiality and protection of personal information on the Internet is very questionable and there are various tools that can be used for network packet tracing and analysis. For instance, Tcpcdump is a command line based packet analyser. It allows the user to truncate and view TCP/IP and other packets transmitted or received over a network to which the computer is connected [23]. Similarly, Netcat is a network utility that can view TC/IP traffic. It was designed as a reliable tool that can be driven directly or easily by other programs and scripts and can be considered as a network debugging and discovery tool with rich features [24].

NetHogs is a small, very useful tool to monitor network traffic by process. It is feature rich, very easy to use and can be easily installed on Linux machines [25]. NetHogs does not rely on a special kernel module to be installed and makes it easy to identify programs that occupy an important portion of the available bandwidth. It can also detect botnets, a number of Internet-connected computers autonomously communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control. Similarly, Interceptor-NG is a versatile network toolkit for a variety of IT professionals. Its main purpose is to save interesting data from network flow and realize different Man-in-the-middle (MITM) attacks [26]. Finally, Ettercap is a comprehensive suite for MITM attacks and host analysis by providing a number of possibilities. It supports active and passive dissection of many protocols and features sniffing of live connections, content filtering on the fly and many other interesting tricks [27].

As well as command line based network packet analysers, there are some web based tools that threaten network security. For instance, SHODAN is a search engine that allows you to find various computer based systems (desktop, switch, router, servers, etc.) using filters [28]. Although it is a search engine, it is very different from search engines like Google, Yahoo or Bing. The search can be done without registration, but if not registered the search will be restricted and filtering will not be possible. Similarly, FOCA (Fingerprinting Organizations with Collected Archives) is a network infrastructure mapping tool and can be used to conduct fingerprinting processes and information gathering on site audit work [29]. These two tools can be used to find out existing video cameras and video chat systems.

As an application designed to access webcam and security cameras, webcamXP is used to access many different webcams and network camera systems [30]. Even if hardware and software access is available, cameras can be moved up and down and up and down. When a camera system is accessed, the services can be

examined using SHODAN. Basically, if there is a system that accesses the camera without asking for a username and password, then it is possible to access the blind spots of the security camera system. It is also possible to find the locations of the houses together with whether they are empty or not. The MAC addresses of the services of those camera systems can also be accessed by whois queries or FOCA queries. Then, those camera systems can be attacked using various techniques such as ARP poisoning via Dynamic Host Configuration Protocol (DHCP) and can be collapsed.

A. Case Study

In this section, the details of how network packets of different software based audio and/or video transmission tools can be traced and analysed are given. It is possible to capture the packets received from/sent to a Skype client. For this purpose, wireshark [31] can be used.

To capture packets sent to/received from a Skype client, firstly, as shown in Fig. 3, device selection is done in the graphical user interface (GUI) of wireshark program. After the device is selected, Start button is clicked to capture the current Skype conversation. It is needed to capture the packets of the whole conversation so that the packets can be analysed. After the conversation is completed, the captured packets can be analysed based on protocols and content. As shown in Fig. 4, the Skype packets captured by the wireshark program belong to either UDP or STUN protocols. As shown in Figs. 5, 6 and 7, detailed information about each captured frame can be viewed. Except for these fields, each UDP packet has content as shown in Fig. 8.

Device	Description
<input type="checkbox"/> Yerel Ağ Bağlantısı* 2	Microsoft
<input type="checkbox"/> Ethernet	Realtek Ethernet Controller
<input type="checkbox"/> Ethernet 3	VMware Virtual Ethernet Adapter
<input type="checkbox"/> VMware Network Adapter VMnet1	VMware Virtual Ethernet Adapter
<input type="checkbox"/> Wi-Fi	Microsoft
<input type="checkbox"/> Bluetooth Ağ Bağlantısı	Microsoft
<input type="checkbox"/> VirtualBox Host-Only Network #2	Oracle
<input type="checkbox"/> Cisco remote capture	
<input type="checkbox"/> Random packet generator	
<input type="checkbox"/> SSH remote capture	

Fig. 3. A list of devices whose traffic can be captured using the wireshark program

```
> Frame 30262: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 2
> Ethernet II, Src: LiteonTe_5a:0f:41, Dst: CiscoInc_9f:11:04
> Internet Protocol Version 4, Src: , Dst:
> User Datagram Protocol, Src Port: 16701, Dst Port: 4315
> Data (75 bytes)
```

Fig. 4. A summary of the captured Skype packets

```

Frame 30262: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 2
Interface id: 2 (\Device\NPF_{A7723D85-086A-4482-819C-FA75DA50D153})
Encapsulation type: Ethernet (1)
Arrival Time: Nov 30, 2016 00:43:55.578183000 Törkiye Standart Saati
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1480455835.578183000 seconds
[Time delta from previous captured frame: 0.001829000 seconds]
[Time delta from previous displayed frame: 0.001829000 seconds]
[Time since reference or first frame: 104.900122000 seconds]
Frame Number: 30262
Frame Length: 117 bytes (936 bits)
Capture Length: 117 bytes (936 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

```

Fig. 5. Frame information

```

0100 .... = Version: 4
... 0101 = Header Length: 20 bytes (5)
v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  0000 00.. = Differentiated Services Codepoint: Default (0)
    .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 103
Identification: 0x2e19 (11801)
v Flags: 0x00
  0... .... = Reserved bit: Not set
  .0. .... = Don't fragment: Not set
  .0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x9825 [validation disabled]
[Header checksum status: Unverified]
Source: [REDACTED]
Destination: [REDACTED]
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]

```

Fig. 6. Detailed IP version 4 information

```

Source Port: 16701
Destination Port: 4315
Length: 83
Checksum: 0x2292 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]

```

Fig. 7. UDP port information

```

Data: 906899510f4ef3616a601a00bede00011222abe1f0cc74e0...
[Length: 75]

00 00 0c f1 f1 04 30 10 b3 5a 0f 41 08 00 45 00 .....0. .Z.A..E.
00 67 2e 19 00 00 40 11 98 25 0a 34 b1 c0 c3 ae .g...@. .%.4....
34 a5 41 3d 10 db 00 53 22 92 90 68 99 51 0f 4e 4.A=...S ".h.Q.M
f3 61 6a 60 1a 00 be de 00 01 12 22 ab e1 f0 cc .a] .....
74 e0 02 3f 67 cd 73 3f 5b a0 f4 c5 5a 40 8b 85 t..?g.s? [...Z@..
f7 07 90 13 93 1b 5c f0 a8 39 e7 7f b7 2b c7 99 .....\. .9...+..
bf a5 a9 f4 7b 52 9b 0d a3 fd 01 e1 a5 b0 3d 61 ....{R. ....=B
16 a1 e9 4e a1 .....N.

```

Fig. 8. Content of a UDP packet

As well as the wireshark program, SHODAN may be used for illegal/unethical purposes. When the website of SHODAN is opened using a browser, it can be used as a search tool to find network cameras around the world as shown in Fig. 9. After the search, information about the selected network cameras can be obtained. As shown in Fig. 10, instead of looking for network cameras, IP address of a webcam or network camera can be typed and then be connected. When the camera is connected, the scene captured by its sensor can be seen, as shown in Fig. 11. As shown in Fig. 12, to obtain further information such as the location of the house, FOCA can be used. FOCA can also be used to view the location of the house as shown in Fig. 13. Please note that the geographical

coordinates of the house were hidden not to lead to undesired acts.

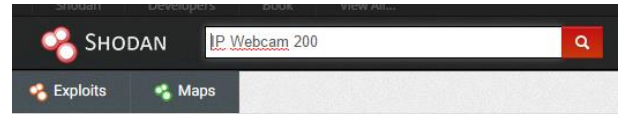


Fig. 9. SHODAN as a search tool

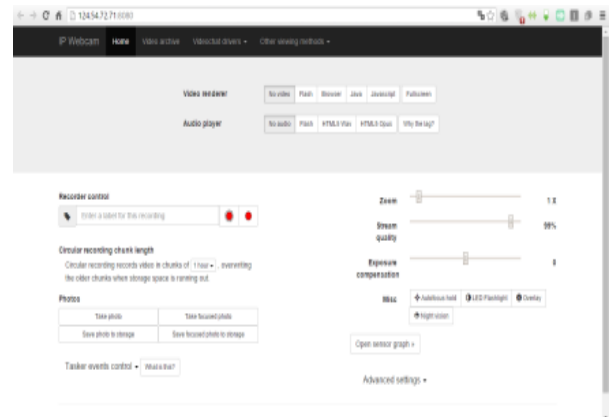


Fig. 10. A camera system whose port 80 is open

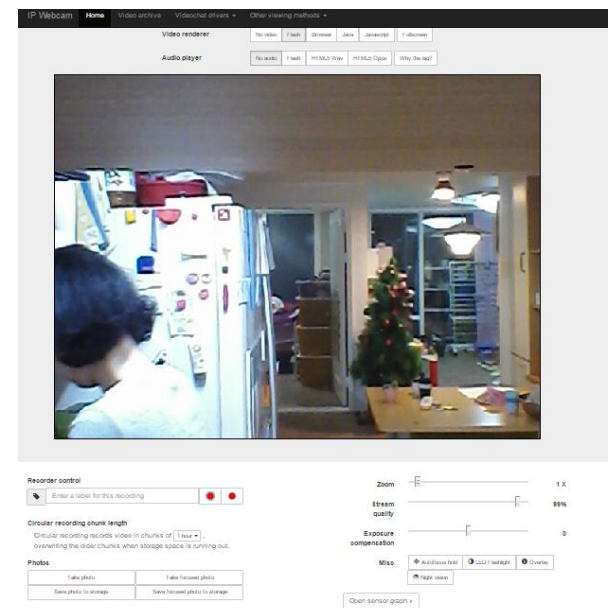
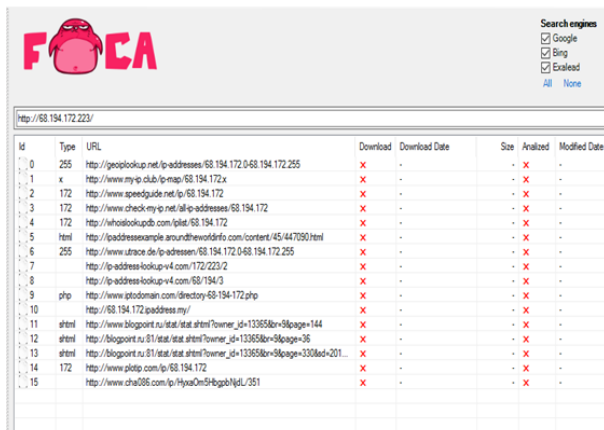


Fig. 11. Viewing the scene captured by the camera



The screenshot shows the FOCA web interface. At the top, there is a search bar and a list of search engines (Google, Bing, Exalead) with checkboxes. Below this, there is a table with columns: ID, Type, URL, Download, Download Date, Size, Analyzed, and Modified Date. The table contains 15 rows of data, each representing a different URL. The 'Download' column shows a red 'X' for each row, indicating that the download was successful. The 'Download Date' column shows the date of the download. The 'Size' column shows the size of the file. The 'Analyzed' column shows a red 'X' for each row, indicating that the file was analyzed. The 'Modified Date' column shows the date of the last modification.

ID	Type	URL	Download	Download Date	Size	Analyzed	Modified Date
0	255	http://geoplookup.net/ip-addresses/68.194.172.0-68.194.172.255	X	-	-	X	-
1	x	http://www.my-ip.club/ipmap/68.194.172.x	X	-	-	X	-
2	172	http://www.speedguide.net/ip/68.194.172	X	-	-	X	-
3	172	http://www.check-my-ip.net/all-ip-addresses/68.194.172	X	-	-	X	-
4	172	http://whoislookupdb.com/ip/68.194.172	X	-	-	X	-
5	html	http://ipaddresssample.aroundtheworldinfo.com/content/45/447090.html	X	-	-	X	-
6	255	http://www.utrace.de/ip-adressen/68.194.172.0-68.194.172.255	X	-	-	X	-
7		http://ip-address-lookup-v4.com/172/223/2	X	-	-	X	-
8		http://ip-address-lookup-v4.com/68/194/3	X	-	-	X	-
9	php	http://www.ipdomain.com/directory/68-194-172.php	X	-	-	X	-
10		http://68.194.172.ipaddress.my/	X	-	-	X	-
11	html	http://www.blogpost.ru/stat/stat.shtml?owner_id=133658&v=9&page=144	X	-	-	X	-
12	html	http://www.blogpost.ru/81/stat/stat.shtml?owner_id=133658&v=9&page=36	X	-	-	X	-
13	html	http://blogpost.ru/81/stat/stat.shtml?owner_id=133658&v=9&page=330&id=201...	X	-	-	X	-
14	172	http://www.platip.com/ip/68.194.172	X	-	-	X	-
15		http://www.cha086.com/ip/4/68/194/3/351	X	-	-	X	-

Fig. 12. Using FOCA to obtain location information

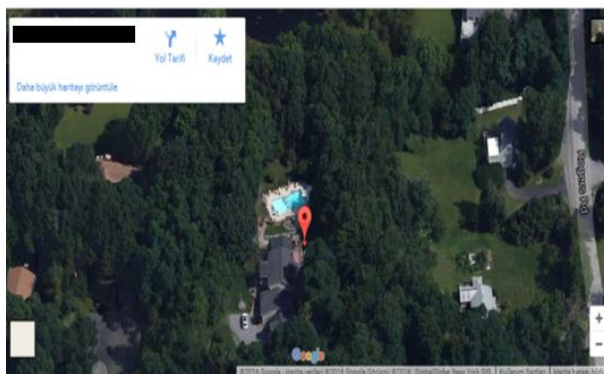


Fig. 13. Location of the house

IV. CONCLUSION

Although people think that their real identity on public networks such as the internet is not revealed, the confidentiality and protection of this information is very questionable. In this study, a case study was realized to show how network packets coming from/sent to IP cameras are traced and analysed with Wireshark program. In addition, how the location information can be obtained was shown. The case study shows that there is a high potential that personal information which should be kept private may be captured and used for illegal purposes.

REFERENCES

- [1] R. Howard and B.J. Jansen, "A proxy server experiment: an indication of the changing nature of the Web," In Proceedings of the 7th International Conference on Computer Communications and Networks, Oct. 15, 1998.
- [2] S. Khanvilkar and A. Khokhar, "Virtual private networks: an overview with performance evaluation," IEEE Communications Magazine, vol. 42, no. 10, pp. 146-154, Oct. 2004.
- [3] C. P. Ruppel and S. J. Harrington, "Sharing knowledge through intranets: a study of organizational culture and intranet implementation," IEEE Transactions on Professional Communication, vol. 44, no. 1, pp. 37-52, 2001.
- [4] C. Metz, "The latest in virtual private networks: part I," IEEE Internet Computing, vol. 7, no. 1, pp. 87-91, 2003.

- [5] J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach (5th ed.). Boston, MA: Pearson Education, 2010.
- [6] Internet: <https://tools.ietf.org/html/rfc768>
- [7] K. J. Connolly, Law of Internet Security and Privacy. Aspen Publishers. p. 131, 2003.
- [8] Internet: <https://tools.ietf.org/html/rfc5389>
- [9] Ilya Grigorik, High Performance Browser Networking: What every web developer should know about networking and web performance. O'Reilly Media, Sebastopol, CA, 2013.
- [10] A. B. Johnston, SIP: Understanding the Session Initiation Protocol, Second Edition. Artech House, 2004.
- [11] Internet: <https://tools.ietf.org/html/rfc3261>
- [12] <https://tools.ietf.org/html/rfc5128#section-3.3>
- [13] C. Booth, "Chapter 2: IP Phones, Software VoIP, and Integrated and Mobile VoIP," Library Technology Reports, vol. 46, no. 5, pp. 11-19, 2010.
- [14] <https://tools.ietf.org/html/rfc2805>
- [15] M. Arjona Ramírez and M. Minami, "Technology and standards for low-bit-rate vocoding methods," in The Handbook of Computer Networks, H. Bidgoli, Ed., New York: Wiley, 2011, vol. 2, pp. 447-467.
- [16] M. Arjona Ramírez and M. Minami, "Low bit rate speech coding," in Wiley Encyclopedia of Telecommunications, J. G. Proakis, Ed., New York: Wiley, 2003, vol. 3, pp. 1299-1308.
- [17] P. Kroon, "Evaluation of speech coders," in Speech Coding and Synthesis, W. Bastiaan Kleijn and K. K. Paliwal, Ed., Amsterdam: Elsevier Science, 1995, pp. 467-494.
- [18] Sipro Lab Telecom (2007-10-25). "FAQ G.729 and G.723.1"
- [19] US Patent 5717825 Algebraic code-excited linear prediction speech coding method, 10th February 1998.
- [20] "Getting started". Microsoft. Retrieved 23 November 2016.
- [21] H. Max, "Skype: The Definitive Guide". Que Publishing. Retrieved 2006-08-22.
- [22] S. A. Baset and H. G. Schulzrinne, "An analysis of the Skype peer-to-peer Internet telephony protocol," In Proceedings of the 25th IEEE International Conference on Computer Communications (IEEE INFOCOM 2006), pp. 1-11, 2006.
- [23] Internet: http://www.tcpdump.org/tcpdump_man.html
- [24] Internet: <http://netcat.sourceforge.net/>
- [25] Internet: <http://nethogs.sourceforge.net/>
- [26] Internet: <https://intercepter-ng.com>
- [27] Internet: <https://ettercap.github.io/ettercap>
- [28] Internet: <https://www.shodan.io/>
- [29] Internet: <https://www.elevenpaths.com/labstools/foca/index.html>
- [30] Internet: <http://www.webcamxp.com/>
- [31] Internet: <https://www.wireshark.org/>