NAME: KALPANA

REG NO: 11903500

SECTION: KE016

ROLL NO: A-09

SUBJECT: OPEN-SOURCE TECHNOLOGIES (INT-301)

GITHUB LINK:

QUESTION NUMBER – 36

PROBLEM STATEMENT: Using any Open Source Software transfer the files from server to client. Explore other options of this open source software.

INDEX

CHAPTER -1 INTRODUCTION

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

TYPES:

- Disk Forensics: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- Network Forensics: It is a sub-branch of Computer Forensics that involves monitoring and analyzing computer network traffic.
- Database Forensics: It deals with the study and examination of databases and their related metadata.
- Malware Forensics: It deals with the identification of suspicious code and studying viruses, worms, etc.
- Email Forensics: It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- Memory Forensics: Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
- Mobile Phone Forensics: It deals with the examination and analysis of phones and smartphones and helps to retrieve contacts , call logs, incoming, and outgoing SMS, etc., and other data present in it. The project that I am doing is under Network Forensics and we will study it now.

Network forensics is the process of analyzing and investigating network traffic to gather information about security incidents or any violations, or events that have occurred on a computer network. This involves capturing data packets and analyzing, logs, and other network traffic to determine the nature of an attack and to what extent an attack happened, and to identify the source of the problem. It can help organizations to understand how a security breach occurred and what data was compromised, and how to prevent similar incidents from happening in the future. It is the main component of computer and network security and is used by law enforcement agencies, businesses, and other organizations to investigate and solve crimes and other security incidents that have happened. Law enforcement will use network forensics to analyze network traffic data harvested from a network suspected of being used in criminal activity or a cyber-attack. Analysts will search for data that points towards human communication, manipulation of files, and the use of certain keywords. Unlike digital forensics, network forensics is more difficult to carry out as data is often transmitted across the network and then lost; in computer forensics data is more often kept in disk or solid-state storage making it easier to obtain.

1.1 OBJECTIVE OF THE PROJECT

The objective of the project is to use Open Source Software transfer the files from server to client. The objective of the project is also that we can explore various open source for transfer the file from server to the client.

1.2 DESCRIPTION OF THE PROJECT

This project involves the transfer of the file from server to client using open source File transfer protocol and is the network used to transfer file between the servers.

It is primarily used for :-

- **Backup** – FTP allows users to backup data and files from one location to a secure server.
- **Duplication** – FTP is a superb way to duplicate data and files from one system to another.
- **Data loading** – FTP is often used to access web hosting services and assists with loading data and files on to a remote system.
- Open source like File drop, LinShare, FileZilla can used to transfer the file from server to the client. By analyzing file transfer, users can gain a better understanding of how their file transfer and operates and identify areas for improvement. In this project we used FileZilla to determine the transfer of the file from server to client.

1.3   SCOPE OF THE PROJECT

The scope of using an open-source software tool is quite broad. Such software can be used to monitor and analyze various aspects of transfer files, including:

- **FTP Secure (FTPS)** – this form of FTP uses Transport Layer Security (TLS) upon connection and is a more secure way of sending and receiving files, with IDs, passwords and certificates in place to verify system authenticity
- **Secure FTP (SFTP)** –SFTP provides a mechanism within Secure Shell (SSH) protocol, using algorithms and encryption to secure data, alongside IDs, passwords and SHH keys to verify authenticity.
- FTP made handling data across the Internet much easier and intuitive. Without FTP and its later iterations, we would not be able to easily stream video content, use video calls, play online games, share files, or enjoy cloud storage. Today, FTP operates behind the scenes as a backbone for data transfer from servers around the world to millions of clients every second of every day.

File transfer protocol is one of many different protocols that dictate how computers and computing systems behave on the Internet. Other such protocols include the following:

- **Hypertext Transfer Protocol (HTTP):** Designed to transmit data across the web
- **Internet Message Access Protocol (IMAP):** Provides access to bulletin board or email messages from a shared service
- **Network Time Protocol (NTP):** Synchronizes clock times on computers over a network.
- FTP enables computers on the Internet to transfer files back and forth. As such, it is an essential tool for those building and maintaining websites today.

Overall, using file transfer software is an effective way for transfer of files between server to client , security professionals, and anyone who wants to understand they can use the open source for transfer of file.

CHAPTER-2 SYSTEM AND SOFTWARE DESCRIPTION

2.1 TARGET SYSTEM DESCRIPTION

To transfer the file from server to client , the target system must have a server as well as client interface that is capable of transfer the file between server to client using open software . The target system must have software installed that can transfer the file. In addition, the target system must also have sufficient system resources, including CPU, memory, and storage, to handle the data and analysis the process of file transfer.

2.2 ASSUMPTIONS AND DEPENDENCIES:

There are several assumptions and dependencies that we need to consider. These include that we need to have access to the file, a compatible network interface, sufficient system resources, proper configuration of the software, knowledge of file transfer protocols and tools, and the time and expertise to carry out the process.

2.3 FUNCTIONAL/NON-FUNCTIONAL DEPENDENCIES:

Functional dependencies are those that relate to the features and capabilities of the open-source software we plan to use. Some of them are with the file transfer between server to client , And support the file transfer protocols, Ability to transfer the files , Ease of use. Non-functional dependencies are those that relate to the operational and performance requirements of the open-source software. Some non-functional dependencies to consider include System requirements, Performance and scalability, Security, Support and community.

**2.4 SOFTWARE DESCRIPTION**:

FILEZILLA

FileZilla is a free, open source file transfer protocol (FTP) software tool that allows users to set up FTP Server or connect to other FTP servers in order to exchange files. FileZilla traditionally supported File Transfer Protocol over Transport Layer Security (FTPS). The client software for FileZilla is available for all platforms and is free. Unlike the commonly chosen alternative form of security in FTP, secure file transport protocol (SFTP), FTPS is less firewall-friendly and requires the opening of a number of ports for its operation. For those who have security requirements for SFTP, previously a secondary client was required but the security has been updated to include both options. Setting up a server in FileZilla is simple, although it is only supported on Windows platforms. To create a new server site, a user downloads the software, opens it and goes to the file menu. In the file menu one chooses site manager. One provides the host name, type of FTP protocol, login method and change from passive connection if required.

CHAPTER-3 ANALYSIS REPORT

3.1 SYSTEM SNAPSHOTS AND REPORT:

In this report, we will discuss the network traffic analysis of my system using FileZilla. FileZilla is a free, open source file transfer protocol (FTP) software tool that allows users to set up FTP Server or connect to other FTP servers in order to exchange files. We will go through the steps of using FileZilla to capture and analyze the transfer of file from server to client in our system.
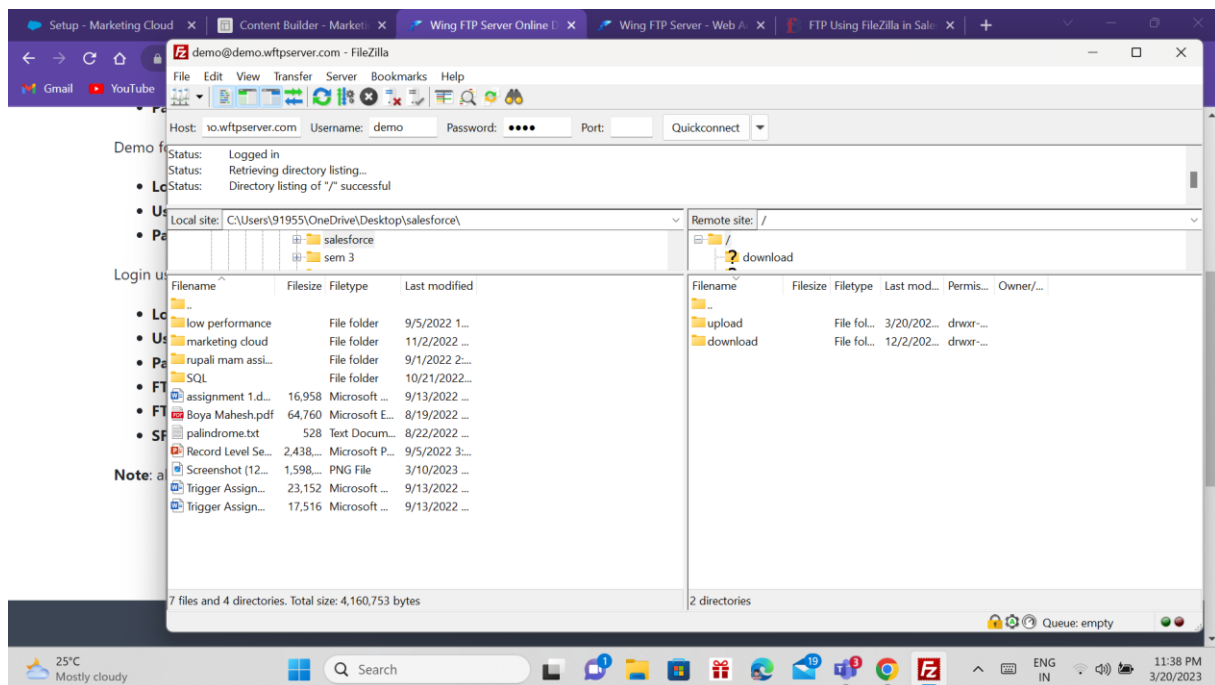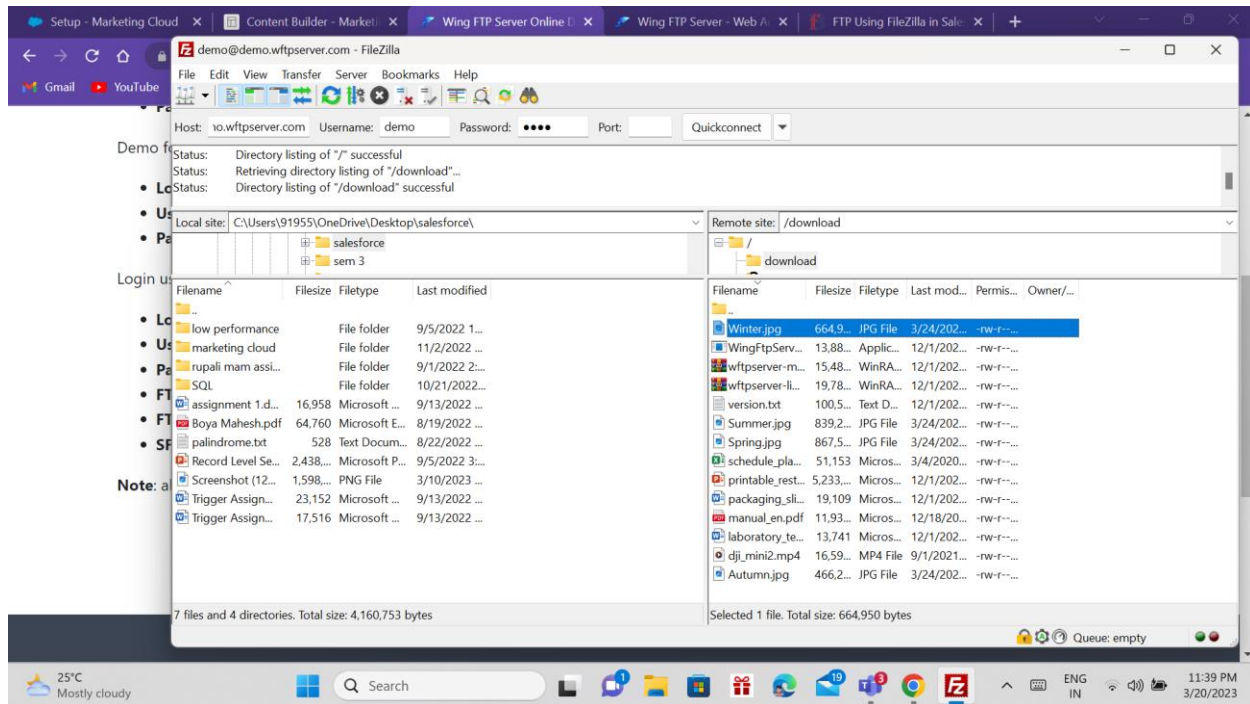
Step 1 :-   DEMO SERVER OF FTP
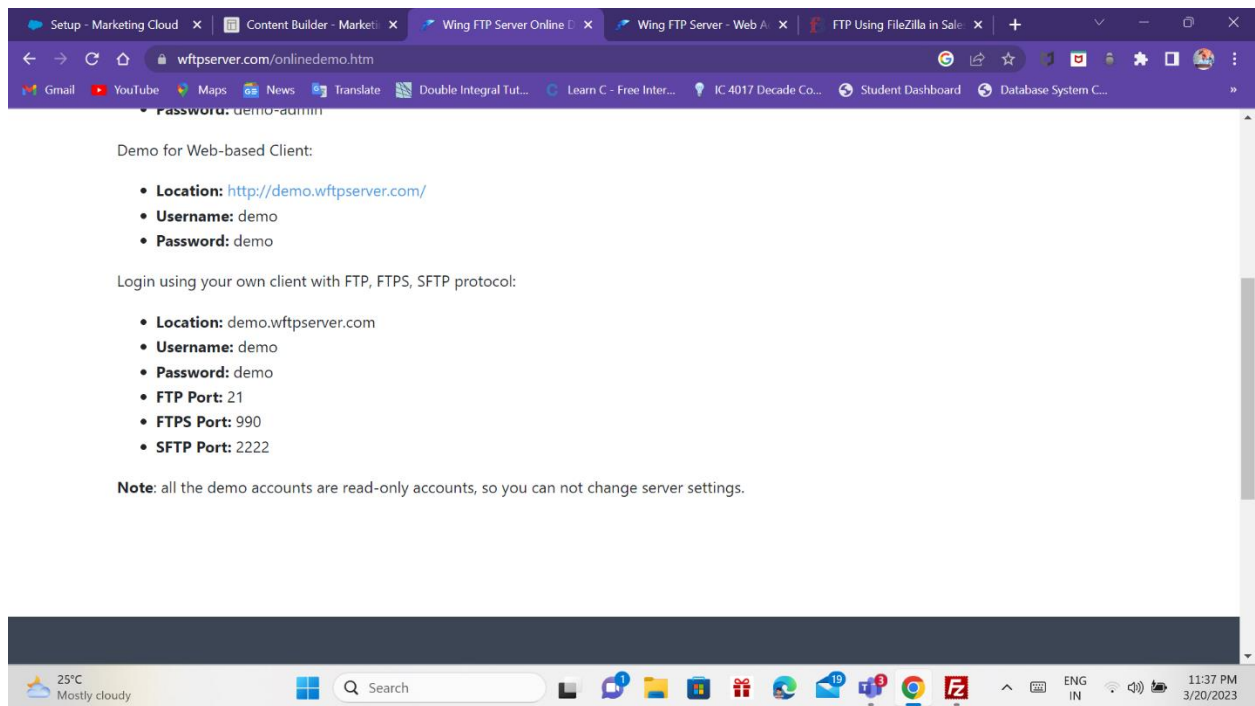
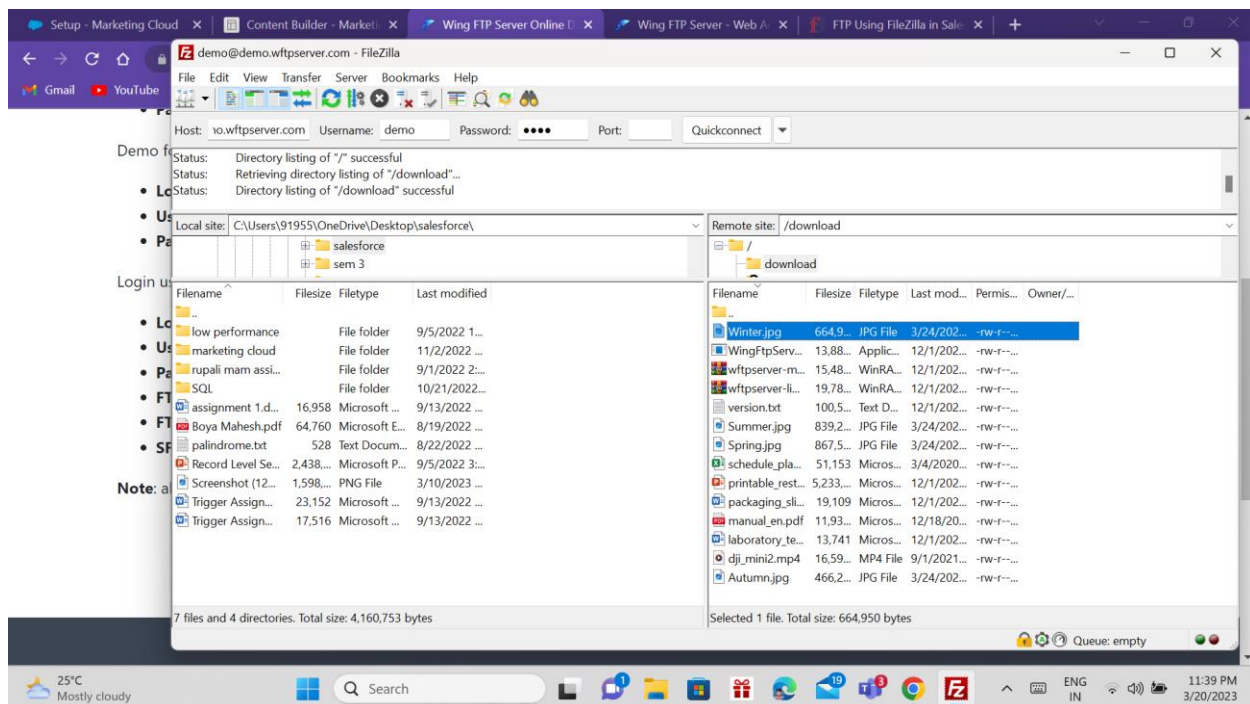**Step 2:- Fill the host , username password and port**
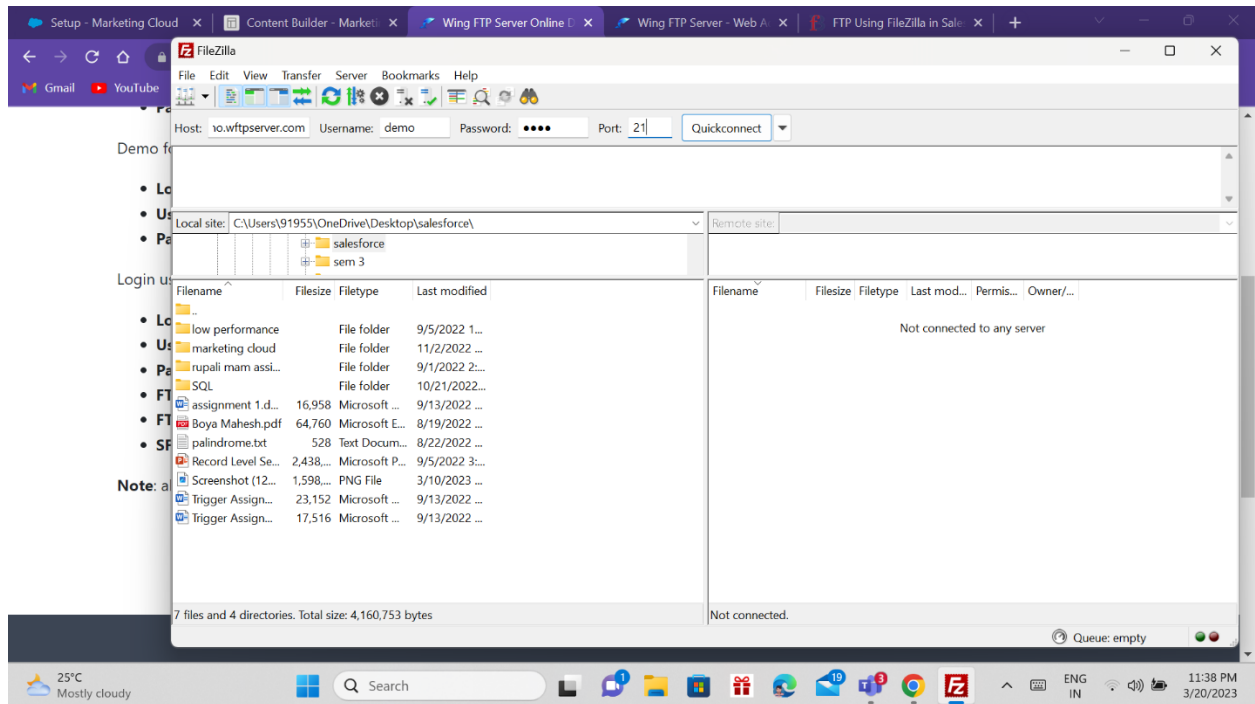
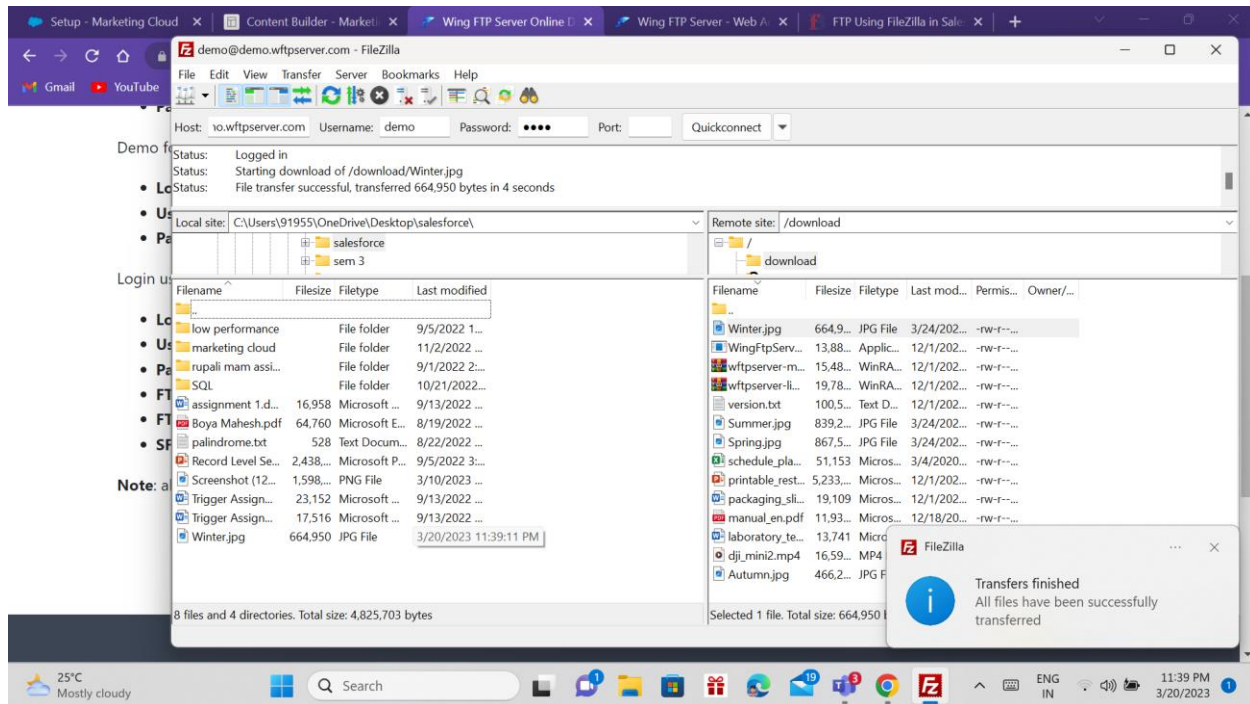**Step 3:- Connection will be created between local and demo system**

Step 4:- Example- transferring the file winter.jpg to local storage

Step 5:- We can drag the file to local and even we can transfer (FTPs,FTP)

Step6:- File has been transfer to local system.

CHAPTER-4 CONCLUSION

In conclusion, capturing and analyzing file transfer protocol using open-source software can be useful for FTP administrators and security professionals. With the right tools and expertise, it is possible to gain insights into file transfer protocol, and optimize file transfer process and performance. However, it is efficient to consider the assumptions, functional dependencies, and non-functional dependencies when working on such a project. FileZilla is an essential tool for file transfer between server to client. It allows us to capture and analyze file transfer protocol in real-time. In this report, we discussed the steps of using FileZilla to capture and analyze FTP in our system. I hope this report has provided you with a good understanding of File transfer Protocol using Filezilla.

REFERENCES:

[1] https://www.techtarget.com/searchsecurity/definition/computer-forensics

[2] https://www.techtarget.com/whatis/definition

[3] https://www.cybrary.it/blog/0p3n/introduction-to-computer-forensics/

[4] https://www.researchgate.net/publication/335015436

[5] https://www.investopedia.com/terms/f/ftp-file-transfer-protocol.asp#toc-types-of-ftp