

Related Topics of Interest

15

INFORMATION IN THIS CHAPTER

- Introduction
- Cryptography
- Data recovery
- IRC
- Bitcoin

INTRODUCTION

In previous chapters we have learned about various topics which are associated to collecting and making sense out of data. We learned about social media, search engines, metadata, dark web, and much more. In this last chapter we will cover some topics briefly which are not directly related to open source intelligence (OSINT) but to the computing and internet culture and its evolution. If you practice the information provided in previous chapters it is very likely to encounter these topics somewhere.

CRYPTOGRAPHY

There has always been a need to transfer messages from one location to another. Earlier people used to send messages through messengers who used to travel long distances to deliver them. Slowly a need to make this transmission secure came up. In situations like war, the message being intercepted by the enemy could have changed the whole situation. To tackle such scenarios people started to invent techniques to conceal the original message, so that even if the message is intercepted it cannot be understood by anyone except the desired receiver. One of the simplest examples is Caesar cipher, in which each letter is replaced by another with a fixed alphabet position difference, so if the position difference is 4 (right), then A would become E, B would become F, and so on. In modern era, technology has advanced a lot and so has the techniques to encrypt as well as break it.

BASIC TYPES

Symmetric key

In this type of cryptography both the parties (sender and receiver) use same key to encrypt and decrypt the message. A popular symmetric key algorithm is Data Encryption Standard (DES), there are also its modern variants such as Triple DES.

Asymmetric key

In this type, there are two keys, public and private. As the name suggests the public key is openly distributed but the private key remains secret. The public key is used to encrypt the message whereas only private key can decrypt it. This solved a major issue with symmetric key which was the need of multiple keys for communication with different parties. RSA is a good example of asymmetric key algorithm.

Some other associated terms:

Hashing

In simpler terms hashing is converting a character string into a fixed size value. Usually the hash is of small length. Some commonly used hashing algorithms are MD5, SHA1 etc.

Encoding

It is simply about converting a character into another form for the purpose of data transmission, storage etc. It is simply like translating a language into another so that the other party can understand it. Commonly used encodings are UTF-8, US-ASCII etc.

The basic difference between these is that encrypted text requires a key to be converted back to plain text and it is mainly used for the confidentiality of message. In hashing, the hashed text cannot be reversed back to the original text and it is mainly used for integrity check and validation. The encoded text can be decoded back with any key.

We came across different examples, cases, scenarios where we learned how data or information plays a vital role in this digital world. Similarly any digital data stored in devices such as computer, laptop, mobile device etc., are equally important. As these are the personal devices, it consists of more personal data so should be taken care of carefully. Any hardware issue, software malfunction, device crash or theft lead to either losing of those important data or can be in wrong hands and the consequences are much worst. So storing any important data in digital form requires a meaningful effort to make that secure. There are many solutions available both open source as well as commercial to store the data securely in these devices. Choose any of those based on the level of confidentiality of data. Apart from storing the data securely and locally in any device there are other cloud solutions available to store our data in one place so that we can retrieve and use those as per our desire. Along with the data storage and data transmission it is also recommended to use secured backup from time to time to avoid any accidental loss of data. The solutions are tightly based on what we learned above and that is cryptography or encryption. Today we frequently use cryptography on daily basis through technologies such as SSL/TLS, PGP, digital signature, disk encryption etc. So here we can conclude that encryption plays a vital role in our day to day life to secure our digital or virtual life.

With increase in computation power the ability to crack encrypted messages have also evolved. Attacks such as Brute-force, dictionary attack are easy to perform at a high speed. Also there are weaknesses in the algorithms, which make it easy

to perform cryptanalysis on them. Given enough time and computation power any encrypted text can be decrypted, so today the algorithms used attempt to make it so time consuming to that the decrypted text becomes worthless in the time used to crack it.

DATA RECOVERY/SHREDDING

Due to technological advancement now a days we prefer to store almost everything in digital form. A person who needs to send his/her documents does not want to visit a photocopy shop. He/she just wants to scan the hard copy for once and use the same soft copy number of time. This is just a simple example to understand human behavior now a days. So storing of important data in soft copy or in digital form arises some of the security risks. As we discussed above, the damage of the device, accidental delete can lead to loss of our important data. We just learned some precautions or in simple what to do with the digital data. But what if it got deleted?

There are possible ways to recover it. For a naive user, data recovery is only possible when the data is still present in trash or recycle bin, but it's not so. The capability of data recovery is way beyond that. This is just because of the very nature of data storage and deletion function implemented by the operating system. To understand this we must understand the basic fundamental of data storage or how data getting stored in different storage devices.

There are different types of storage devices such as tape drives, magnetic storage devices, optical storage devices, and chips. Tape drives are not generally used for personal use, earlier it was an integral part of the enterprise storage system, now there is a possibility that it is being deprecated so let's not talk about that. Apart from tape drive the other three are widely used. Magnetic devices are nothing but the hard disk devices we use, popularly known as HDD or hard disk drive, which stores all the data. When we delete data from our system the operating system does not delete the data from the magnetic disk but it just remove the address reference to that part, from the address table. Though the concept will be quite the same for all other media types such as DVD, but as we use these storage devices for backup and the HDDs for general storage, we will focus on HDD only. As we discussed that deleting a data from the system means removing its memory location details from the address table. So what is an address table and how it works? It's quite simple. Generally when we store the data in device it takes some memory from the HDD. The starting memory location and the ending memory location define a data in hard disk. All these memory location details are stored in a table called address table. So when we search for a particular data the system checks the address table to get the memory locations allocated for that. Once it gets that memory location it retrieves the data for us. As after deleting the data, the data is still present in the hard disk; we can recover it, unless it is overwritten by other data. Here deleting means deleting data from system as well as trash or recycle bin. So now we have some idea why data can be recovered after deletion but the major question still stands is how? Let's take a look into that as well.

There are many tools available on internet to recover deleted files from different operating systems, some are free and some are paid. The recovery process is quite easy. Install the software in the operating system and then open the application. Generally all the recovery tools come with a simple user friendly GUI or graphical user interface. Follow simple instructions and complete the wizard to recover the data successfully.

Wise Data Recovery is a good example of such tools, which can be downloaded from <http://www.wisecleaner.com/wisedatarecoveryfree.html>. The installation is simple and usage is pretty straightforward. Simply select the drive to be scanned for file recovery. Once the files are listed with their recoverability status we can select them and click on Recover button at the bottom right to perform the operation.

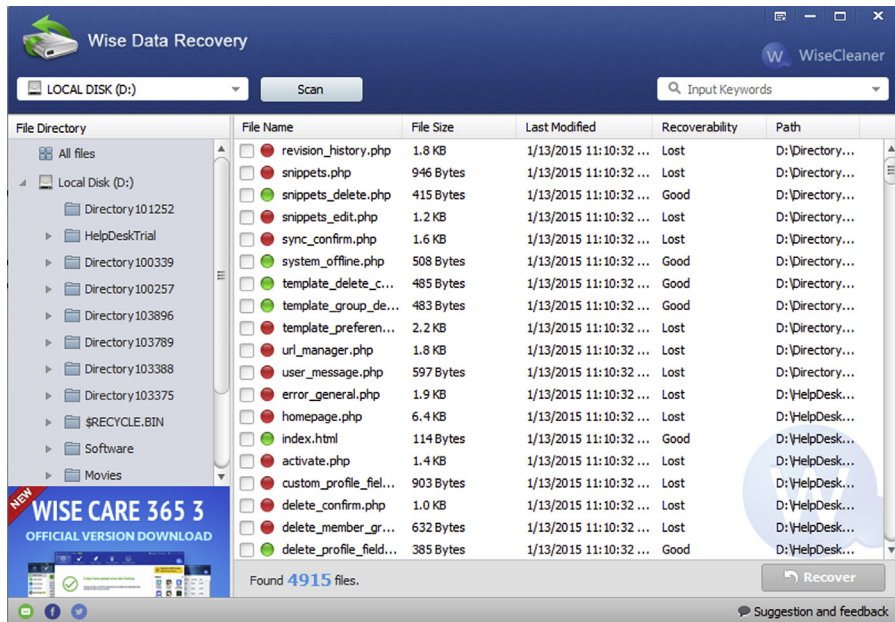


FIGURE 15.1

Data recovery using Wise Data.

Now as we know that sometimes it is possible to recover the data we have deleted, we should also know there are tools which can actually delete data from the disk. One such tool is FileShredder available at <http://www.fileshredder.org/>.

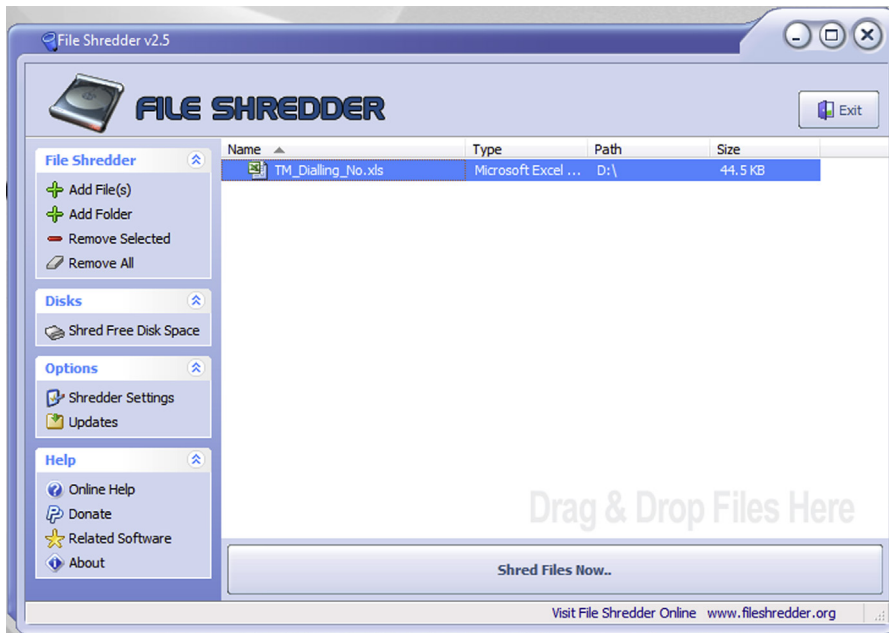


FIGURE 15.2

Data shredding using FileShredder.

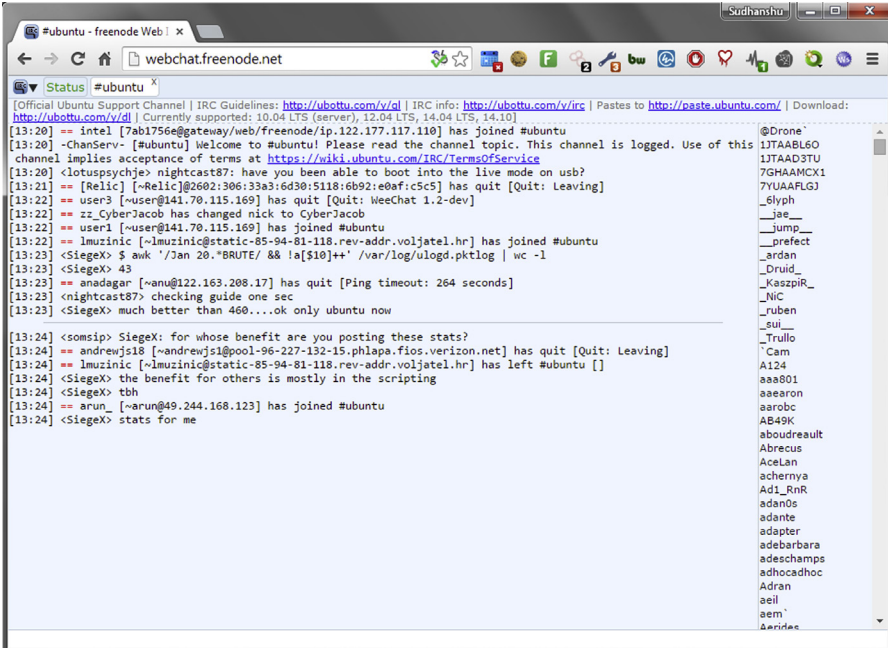
INTERNET RELAY CHAT

IRC or the Internet Relay Chat is like old school for many. It was developed by Jarkko Oikarinen in late 1980s. Though it was developed two decade back but the popularity of this application is still there. People still love to use IRC. The statistical data says it lost half of its users in last decade but as per a product of this old if still people are willing to use it's a great achievement.

IRC is quite same as any other chat application. It follows client server architecture and uses TCP protocol for communication. Earlier it uses plain text communication but now it also supports TLS or Transport Layer Security for encrypted communication. The major reason for its development was to use it as a group chat software and it serves the purpose quite well. As in general term we say different types of chat groups as chat room. In IRC terms it is called as channel. Unlike other chat clients it does not force a user to register but a user has to provide a nickname to start chatting. A user can chat in channel as well as directly with another user using private message option. IRC is widely used in different discussion forums and we love to use this whenever we get an opportunity to use.

Normally to use IRC we need to install an IRC client in our system. There many clients available in internet and for all kinds of operating systems. So download a client which supports the operating system being used. Once we get an IRC client installed, connect to a channel to start communicating with fellow channel member.

The chat process is also quite same as the normal chat process. It's basically line-based chat. One user will send a message in a line then the other will reply. Due to its anonymity most hackers prefer the use of IRC. The major question here is how it's going to help us in OSINT. It's quite simple as there are various channels available we can choose one based on our interest and crowdsource our question and get response from different experts. We need to be in the right place in right time to discuss what is happening in the cyber world. We can get clear scenario about what is happening all over the world and, for example, if we are lucky enough then we might get future prediction also such as which group is preparing for a distributed denial-of-service (DDOS) attack on a company, what are the possible targets, what is the current attack vectors hacktivists are using, and many more. The information we will get from here can be used to define cyberspace, trends in cyberspace and future prediction, discuss a query etc. So next time do not hesitate to use IRC, just provide a fancy name and enjoy chatting. A simple web-based IRC platform is <http://webchat.freenode.net/>. Simply enter a nickname and channel name, and start to explore.



```

[Official Ubuntu Support Channel | IRC Guidelines: http://ubuntu.com/y/ol | IRC info: http://ubuntu.com/y/rc | Pastes to http://paste.ubuntu.com/ | Download: http://ubuntu.com/y/d/ | Currently supported: 10.04 LTS (server), 12.04 LTS, 14.04 LTS, 14.10]
[13:20] == intel [7ab1756@gateway/web/freenode/ip.122.177.117.110] has joined #ubuntu
[13:20] == ChanServ- [#ubuntu] Welcome to #ubuntu! Please read the channel topic. This channel is logged. Use of this channel implies acceptance of terms at https://wiki.ubuntu.com/IRC/TermsOfService
[13:20] <lotuspsychje> nightcast87: have you been able to boot into the live mode on usb?
[13:21] == [Relic] [~Relic]@2602:306:33a3:6d30:5118:6b92:e0af:c5c5 has quit [Quit: Leaving]
[13:22] == user9 [-user@141.70.115.169] has quit [quit: WeeChat 1.2-dev]
[13:22] == rz.CyberJacob has changed nick to CyberJacob
[13:22] == user1 [-user@141.70.115.169] has joined #ubuntu
[13:22] == lmuzinic [~lmuzinic@static-85-94-81-118.rev-addr.voljatel.hr] has joined #ubuntu
[13:23] <SiegeX> $ awk '/Jan 20.*BRUTE/ && !a[$10]+' /var/log/ulogd.pktlog | wc -l
[13:23] <SiegeX> 43
[13:23] == anadagar [~anu@122.163.208.17] has quit [Ping timeout: 264 seconds]
[13:23] <nightcast87> checking guide one sec
[13:23] <SiegeX> much better than 460....ok only ubuntu now

[13:24] <somsp> SiegeX: for whose benefit are you posting these stats?
[13:24] == andrewjs18 [-andrewjs1@pool-96-227-132-15.phlpa.fios.verizon.net] has quit [Quit: Leaving]
[13:24] == lmuzinic [~lmuzinic@static-85-94-81-118.rev-addr.voljatel.hr] has left #ubuntu []
[13:24] <SiegeX> the benefit for others is mostly in the scripting
[13:24] <SiegeX> tth
[13:24] == arun_ [-arun@49.244.168.123] has joined #ubuntu
[13:24] <SiegeX> stats for me
  
```

FIGURE 15.3

Freenode IRC.

BITCOIN

Anyone into information security or keeping track of world media especially technical journals must have heard of the term “bitcoin.” It was popular for its new concept earlier in technical field but later when the value of 1 bitcoin touched almost 1000\$, it

started to trend between common internet users. Many must be aware of this but still we will discuss some of the important facts about bitcoin. Bitcoin can be referred as electronic currency or digital cash developed by Satoshi Nakamoto. Unlike normal currencies it uses a decentralized concept called peer-to-peer technology for transactions. It is based on an open source cryptographic protocol in a format of SHA-256 hash in hexadecimal form. The smaller unit of a bitcoin is called as satoshis. 100 million satoshis at a time creates one bitcoin. Bitcoin can also be referred as payment system as there are no banks, organization, or individual has power to control or influence it. It's always in digital form and can be transferred within a click to any individual over the world. There are pros as well as cons for this also. Some of the pros are we can convert bitcoin into any currencies independent of country. We can transit it anonymously, hence it is quite popular in darknet. No one can fake, create, or devalue bitcoins. Similarly there a large amount of cons also such as a transaction cannot be reversed. The security of bitcoin is low as it always there in digital form. Once a bitcoin wallet is deleted it is lost forever.

Now we have a bit understanding on bitcoins. So it's important to know how to store it also. We can store bitcoin digitally only, because it's a digital data. We need a bitcoin wallet to store bitcoin. The major disadvantage of this is once accidentally we delete our wallet, we lose all the money. So take backups in proper intervals to avoid any such incident. The initial bitcoin project site is <http://www.bitcoin.org/>.

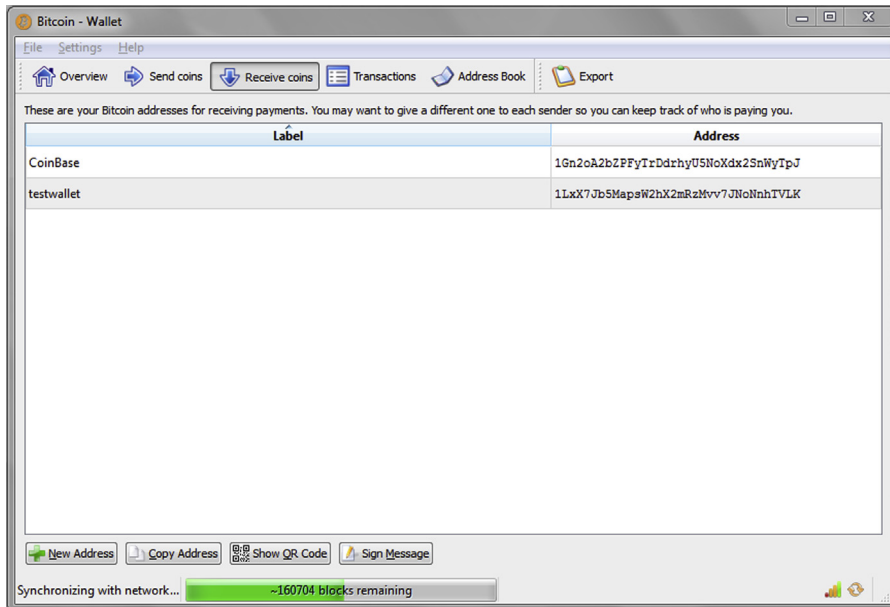


FIGURE 15.4

Bitcoin wallet.

So this is where it all ends. We had a long journey in which we explored a lot of topics, learned about many different tools, techniques, and methods to explore around. In later part we also discussed how and what to do with all this information. We also saw some related scenarios and examples. All in all hopefully we can say that it was a great learning experience at both ends. One important point that needs to be made is that in today's world "Information is Power" and with power comes great responsibility. Use the knowledge gained through this volume for ethical purposes and contribute to create a better world.