1
Understanding the Deep and Dark Web

The Deep Web, the Dark Web, the Dark Net.

We've all heard about them, if it's from a movie, TV show, the news, or even a friend or a neighbor. Most people view them as the same thing, which is as a depraved and illegal area on the internet, where sex-traffickers, drug dealers, weapons dealers, and others lurk in wait for innocent users.

The truth is very far from this. In this book, we'll understand what the Deep Web, the Dark Web, and the Dark Net are, how to access them safely and securely, who uses them and, ultimately, how we can use them for beneficial and good uses, rather than what the media publishes about them.

But, in order to fully understand them, we need to understand the origins of the internet, and how it works, as they are intrinsically connected.

We will cover the following topics in this chapter:

- The origin of the internet
- The Deep Web
- The Dark Web

The origin of the internet

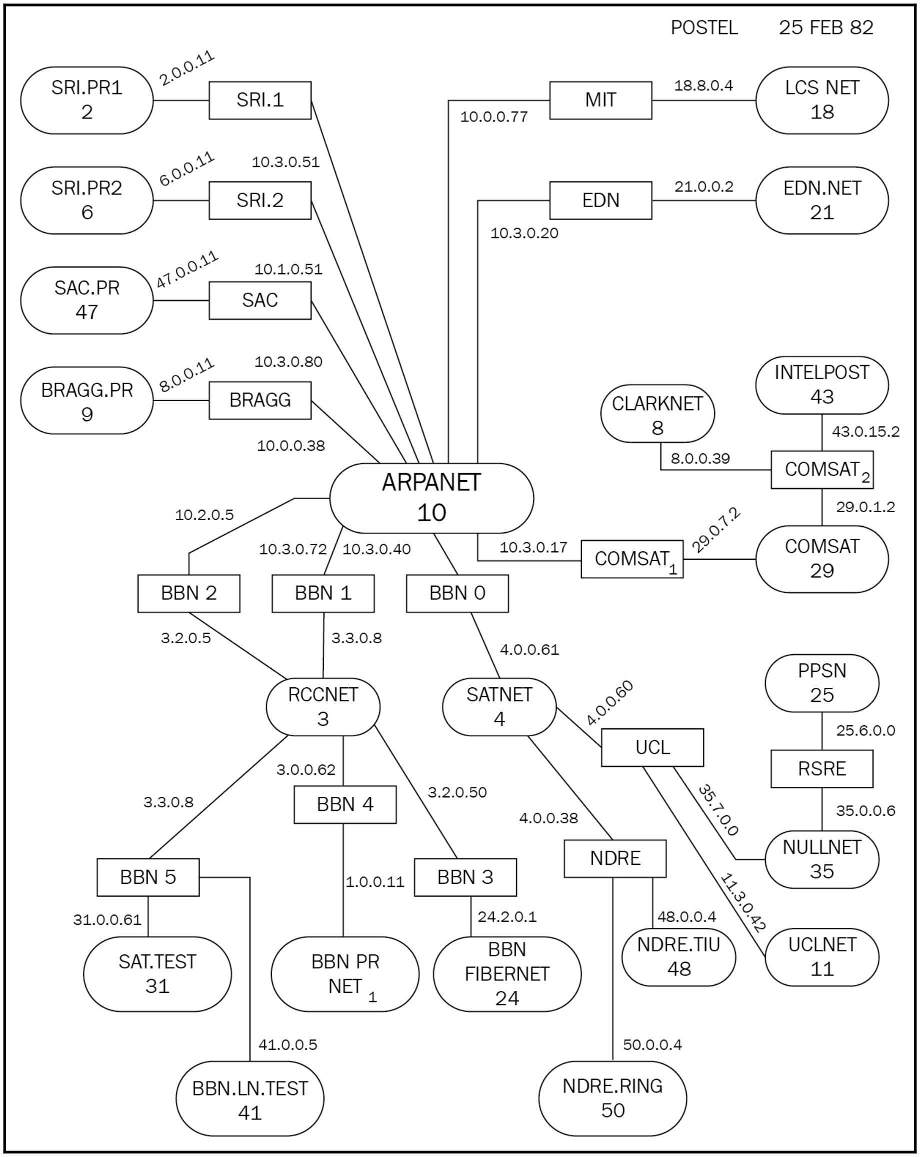
Many of you might have heard that the internet was originally created by DARPA, The Defense Advanced Research Projects Agency, which is part of the United States Department of Defense, and is responsible for development of new technologies for use by the US military.

But, this is not necessarily the first appearance of the internet. Back then, it was more of an **intra**-net, as all the computers were on the same network. It all depends on how you define the internet. Nowadays, the internet is defined as a *network of networks* or multiple interconnected computer networks that provide communication and information capabilities, using standardized communication protocols such as **Transport Control Protocol/Internet Protocol** (**TCP/IP**)

Some say that the internet began after packet switching technology was created, others say it was after TCP/IP was launched, and yet others claim that the origins of the internet were in the UK, not in the US.

The starting date of the internet (or rather ARPANET, as it was known then) is also inconclusive. Although most people agree that it was launched in 1969, there is concrete evidence that it originated even earlier.

The following diagram is a model of ARPANET from 1982:



In August 1962, J.C.R. Licklider of MIT began discussing his *Galactic Network* concept. His idea was to create a globally interconnected set of computers through which anyone could quickly access data and programs from anywhere in the world.

This was based on packet switching technology, a way by which messages can travel from point to point across a network. He even got to the point where he implemented a packet switch connecting a set of host computers. This technology was already a concept in 1965, proposed by an Englishman called Donald Davies, but it never got funded. ARPANET adopted his ideas and continued from there.

Additionally, a Frenchman called Louis Pouzin introduced the idea of datagrams (data + telegram—a basic transfer unit in a packet-switched network) around that time.

In 1968, The National Physical Laboratory in the UK set up the first test network for packet switching. This inspired DARPA to work on ARPANET.

Whatever the origin of the internet, the original intent of ARPANET was to allow people in remote locations to use the processing power of remote computers for scientific calculations.

In December 1970, the initial ARPANET host-to-host protocol, called the **Network Control Protocol** (**NCP**), was added to the network, and in 1972, email technology was introduced.

Additionally, in 1972, the concept of open-architecture networking was introduced, providing the basis for networks of different technologies to be able to connect (this also sowed the seeds for the OSI model in the future).

In 1978, TCP/IPv4 was released, and was added to ARPANET in 1983. This was the first actual internet, the basis of the internet which we know and love today.

So, what is the internet?

As shown in the above diagram, it's a vast, global network of interconnected networks that uses TCP/IP to communicate.

There are literally millions upon millions of networks connected, and nowadays the networks are no longer only computer-based. **internet of Things** (**IoT**) technology connects devices that aren't computers to the internet, as well.

You may also be familiar with the term **World Wide Web**.

Also called simply *the web*, it's a way of accessing information, such as web resources and documents, by accessing **Uniform Resource Locators** (**URLs**) and Hypertext links, using various protocols (such as **Hypertext Transfer Protocol** (**HTTP**)) to allow applications (such as a browser) to access and share information.

A protocol is a set of rules that dictates how to format, transmit, and receive data so network devices can communicate, regardless of their infrastructure, design, or standards.

Browsers were created in 1990 by English scientist Tim Berners-Lee during his employment at CERN, in Switzerland.

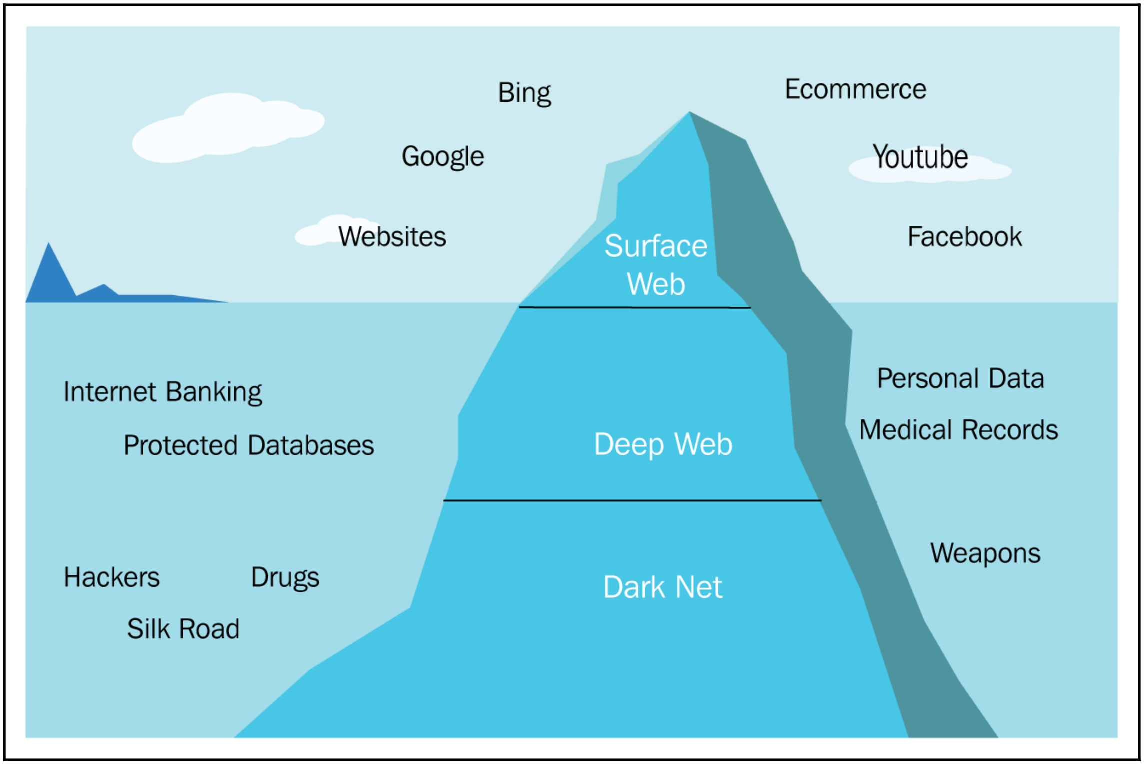
The internet is the infrastructure upon which the World Wide Web can be used.

Now, after we've understood what the internet is and how it began, let's talk about the Deep Web.

As you know, Google and other search engines (Bing, Yahoo, and so on) index sites by *crawling* them and incorporating the data crawled into their index servers. The search engines then organize the data by context, according to their logic, and enter the data into a base of algorithms that make up the search engine.

This data, indexed by a search engine, and accessed via the World Wide Web (also called the Surface Web), is actually only a small part of the entire internet.

Many people like to view the internet as an island or a glacier at sea, and only part of it is viewable above the surface of the water:



Surface Web, Deep Web, and Dark Net

As you can see in the preceding diagram , the Surface Web is the tip that's visible above the water.

This area can be indexed by search engines, and contains all the publicly available information, documents, and content.

Sadly, many people who aren't tech-savvy or aren't aware, and even companies, allow their data to be indexed, which provides information to attackers, helping them gain access, locate files and data, and more.

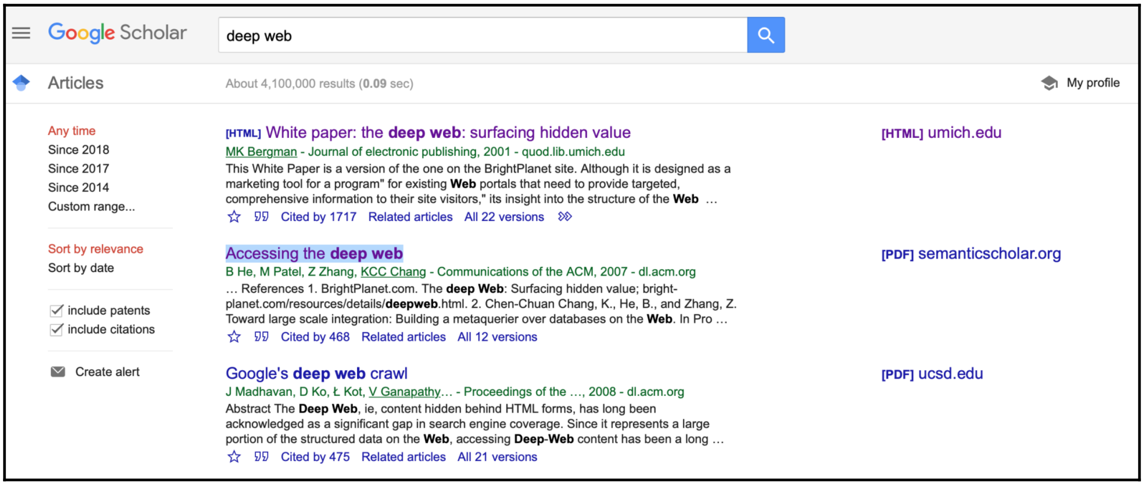
For example, an attacker might want to cause reputational damage to a certain business. Performing reconnaissance, the attacker discovers a weakness to be exploited—the business' backups procedure saves the backup of their customer database to their public website for 24 hours before it is moved to a secure location. This allows the backup to be crawled by search engines. The attacker can use a search engine to find the database file on the business' website. Since the website is indexed, the search engine is able to provide the results to the attacker. The attacker can then simply download and use the file(s) for malicious purposes.

The Deep Web

If the Surface Web is the indexable part of the internet, the Deep Web is everything else. The Deep Web is the area on the internet that can't be, or isn't, indexed. And it's much, much bigger. This is because the Deep Web includes much more than what you probably think. Remember—the internet isn't the World Wide Web (Surface Web). It's the infrastructure over which the Surface Web is accessed. So, the Deep Web (most of it, anyway, but we'll talk about that soon), also exists on the internet. Any website or system that requires login credentials is part of the Deep Web.

Organizational information and intranets of businesses, academic institutes, governmental departments, and others, are also part of the Deep Web, as are websites that specifically prevent search engines from indexing parts of the website, such as Google Scholar, or Amazon.

The following screenshot displays searching for `deep web` in Google Scholar:



deep web

About 4,100,000 results (**0.09** sec)

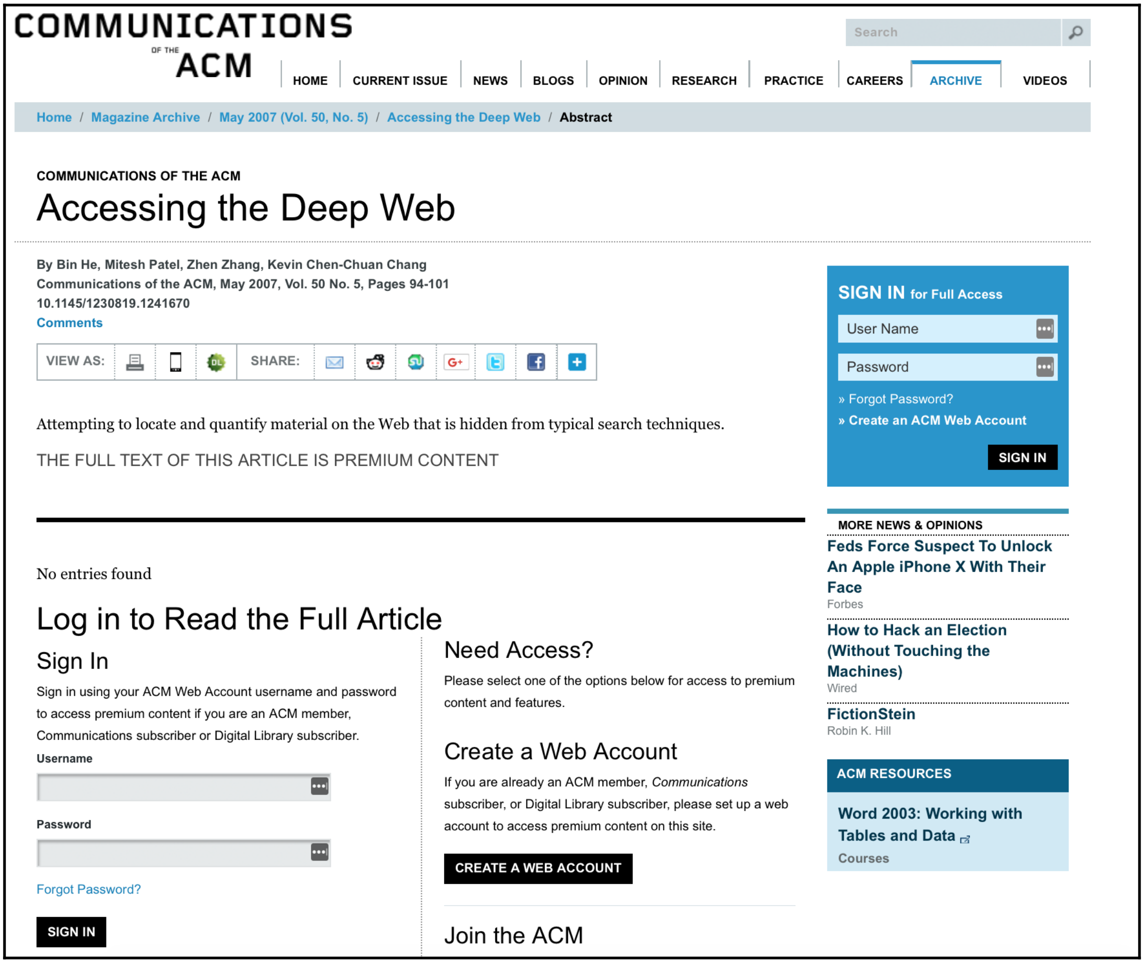
[HTML] White paper: the **deep web**: surfacing hidden value — [HTML] umich.edu
MK Bergman - Journal of electronic publishing, 2001 - quod.lib.umich.edu
This White Paper is a version of the one on the BrightPlanet site. Although it is designed as a marketing tool for a program" for existing **Web** portals that need to provide targeted, comprehensive information to their site visitors," its insight into the structure of the **Web** ...
☆ 99 Cited by 1717 Related articles All 22 versions

Accessing the **deep web** — [PDF] semanticscholar.org
B He, M Patel, Z Zhang, KCC Chang - Communications of the ACM, 2007 - dl.acm.org
... References 1. BrightPlanet.com. The **deep Web**: Surfacing hidden value; bright-planet.com/resources/details/**deepweb**.html. 2. Chen-Chuan Chang, K., He, B., and Zhang, Z. Toward large scale integration: Building a metaquerier over databases on the **Web**. In Pro ...
☆ 99 Cited by 468 Related articles All 12 versions

Google's **deep web** crawl — [PDF] ucsd.edu
J Madhavan, D Ko, Ł Kot, V Ganapathy... - Proceedings of the ..., 2008 - dl.acm.org
Abstract The **Deep Web**, ie, content hidden behind HTML forms, has long been acknowledged as a significant gap in search engine coverage. Since it represents a large portion of the structured data on the **Web**, accessing **Deep-Web** content has been a long ...
☆ 99 Cited by 475 Related articles All 21 versions

As you can see, there are results.

After clicking the **Accessing the deep web** link, note the following:



COMMUNICATIONS OF THE ACM

Accessing the Deep Web

By Bin He, Mitesh Patel, Zhen Zhang, Kevin Chen-Chuan Chang
Communications of the ACM, May 2007, Vol. 50 No. 5, Pages 94-101
10.1145/1230819.1241670
Comments

Attempting to locate and quantify material on the Web that is hidden from typical search techniques.

THE FULL TEXT OF THIS ARTICLE IS PREMIUM CONTENT

No entries found

Log in to Read the Full Article

Sign In

Sign in using your ACM Web Account username and password to access premium content if you are an ACM member, Communications subscriber or Digital Library subscriber.

Username

Password

Need Access?

Please select one of the options below for access to premium content and features.

Create a Web Account

If you are already an ACM member, *Communications* subscriber, or Digital Library subscriber, please set up a web account to access premium content on this site.

Join the ACM

Feds Force Suspect To Unlock An Apple iPhone X With Their Face
Forbes

How to Hack an Election (Without Touching the Machines)
Wired

FictionStein
Robin K. Hill

Word 2003: Working with Tables and Data
Courses

We arrive at a login screen. So, the article itself is on the Deep Web, but its title and metadata was indexed by Google, and therefore was returned as a search result.

Now, let's understand what we just read—the Deep Web is accessible using any standard browser, but is not indexed by search engines, so you usually need to either enter a username and password to access the content or be in a specific network (company or university network, for example).

But what about the Dark Web?

The Dark Web

As the Surface Web, or WWW, is on the internet, the Dark Web exists on the Dark Net (or rather, multiple darknets).

It's important to point out that the terms Dark Web and Dark Net aren't the same thing. Dark Net was a term used in the 1970s', for networks that were isolated from ARPANET, mainly for security purposes, such as compartmentalization. They were configured to be able to receive external data, but they were hidden from the ARPANET network listings and wouldn't respond to networking inquiries, such as ping requests.

Over time, the term was also used for overlay networks, which are essentially networks that utilize software and hardware to create multiple layers of abstraction. These layers are run over multiple separate and discrete network layers on top, or over a common network (hence *overlay*), accessible only with special browsers or software, or where their IP addresses aren't globally routable. A few examples of such overlay networks are Tor, the **Invisible internet Project** (**I2P**), or FreeNet.

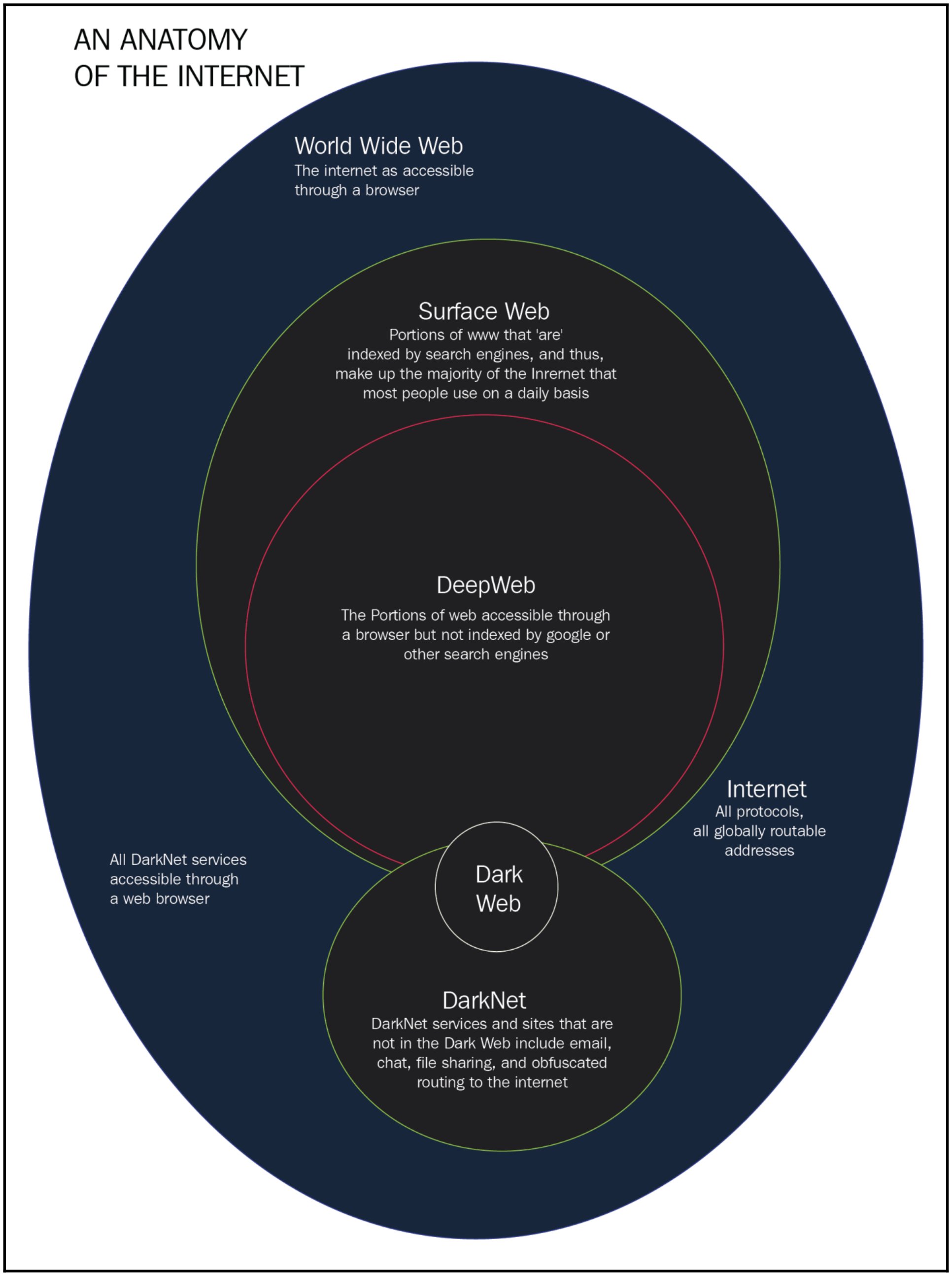
So, you can view the Dark Net as the infrastructure underneath the Dark Web, which is the content and websites that you can access only with the specialized software I mentioned, and which we will discuss as we proceed in this chapter, and in the book.

To give you an example of a Dark Net, I'll mention Tor, or The Onion Router. It's essentially a distributed network of servers or hosts, where users, traffic is bounced around between various routers.

This makes it hard to monitor the data, enhancing anonymity, privacy, and security.

A comparison between TOR and I2P can be found here: `https://geti2p.net/en/comparison/tor`.

The following diagram is from the Argonne National Laboratory website, and it demonstrates what I just mentioned in a graphical manner:


AN ANATOMY
OF THE INTERNET
World Wide Web
The internet as accessible
through a browser
Surface Web
Portions of www that 'are'
indexed by search engines, and thus,
make up the majority of the Inrernet that
most people use on a daily basis
DeepWeb
The Portions of web accessible through
a browser but not indexed by google or
other search engines
Internet
All protocols,
all globally routable
addresses
All DarkNet services
accessible through
a web browser
Dark
Web
DarkNet
DarkNet services and sites that are
not in the Dark Web include email,
chat, file sharing, and obfuscated
routing to the internet

As you can see, the internet encompasses the Deep Web, which is in (or under) the Surface Web, and the Dark Web, which is on the Dark Net (yet another part of that magnificent *network of networks* known as the internet).

We will discuss who uses the Dark Web, and how, in this book, but let's take a high-level look first, before we dive in.

Law enforcement

I'll start with law enforcement, since most people believe that the Dark Web is illegal, either to access, or due to what goes on there. So, I want to reassure you—just as in the real world, so also in the Dark Web do we have law enforcement. Due to its anonymity and privacy, criminals use the Dark Web. And where there are criminals, there are police. Due to the anonymity, criminals can create online marketplaces for drugs, weapons, and other illegal material. Law enforcement agencies such as the FBI and many others utilize the Dark Net for sting operations, to capture criminals. They leverage the Dark Web themselves, reducing the exposure of governmental IP addresses and ensuring their anonymity on the Dark Web, thus increasing their effectiveness.

One of the things that law enforcement agencies do is to take down illegal marketplaces. Many agencies attempt to take over illegal marketplaces, enabling them to not only deter the sale of illegal materials, but to also track the buyers and sellers of such materials.

Journalism

Journalists often need to report a story, only to be at risk for various reasons. Using the Dark Web, journalists are able to report and share information anonymously and securely. Services such as *Secure Drop* exist to enable organizations to receive documents and tips from anonymous sources. There are a number of major news agencies that use Secure Drop.

Secure Drop keeps a directory of active instances, and you can view this here: `https://securedrop.org/directory/`.

Privacy

Privacy is a top concern for many people today. With the rise of interconnected devices and data being moved to the cloud, privacy concerns are on the rise.

When you browse an average website, there are a number of tracking actions that the website can perform. For example, a website can leverage the following:

- Tracking cookies
- Fingerprinting of the browser
- Referral links
- IP addresses
- Tracking scripts

Using the information obtained, websites can perform a few things, such as targeted advertising.

By using the Dark Web, people ensure that they are keeping their legal online activity anonymous. There is no need to worry about websites tracking your location or online activity.

Criminals

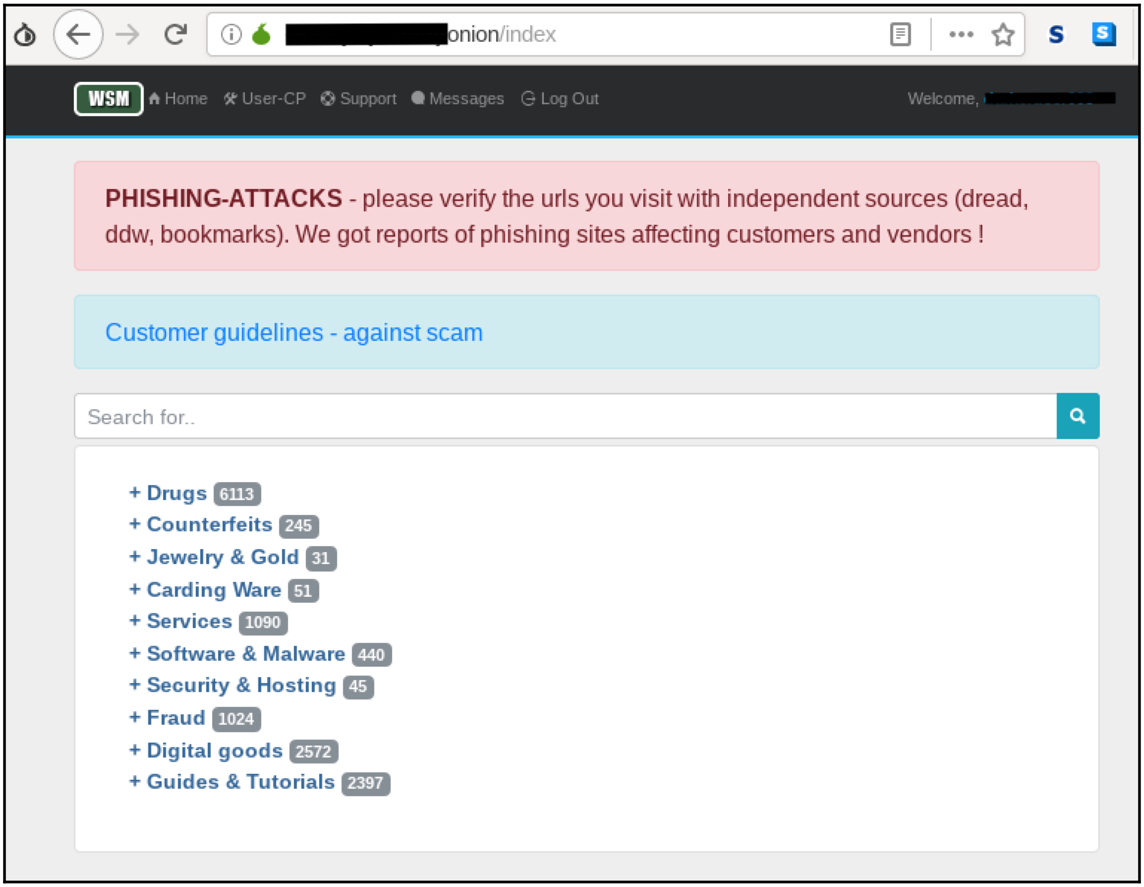
Since the Dark Web offers anonymity and security, criminals often use it to protect themselves and to prevent capture. Although law enforcement agencies operate within the Dark Web, it does mean that they stop all criminals from partaking in criminal activities.

Drugs and illegal substances

There are a variety of marketplaces within the dark web that sell a vast array of drugs and illegal substances. One of the most popular marketplaces is *Silk Road*.

Silk Road started back in 2011 and was used to sell magic mushrooms at first. The marketplace started to grow and moved on towards other drugs and commodities. Silk Road has progressed to version 3.1. The previous versions were also taken down either by law enforcement or by the admins.

Another marketplace that is very popular is the *Wallstreet Market*. This marketplace offers a variety of goods, as can be seen here:



PHISHING-ATTACKS - please verify the urls you visit with independent sources (dread, ddw, bookmarks). We got reports of phishing sites affecting customers and vendors !

Customer guidelines - against scam

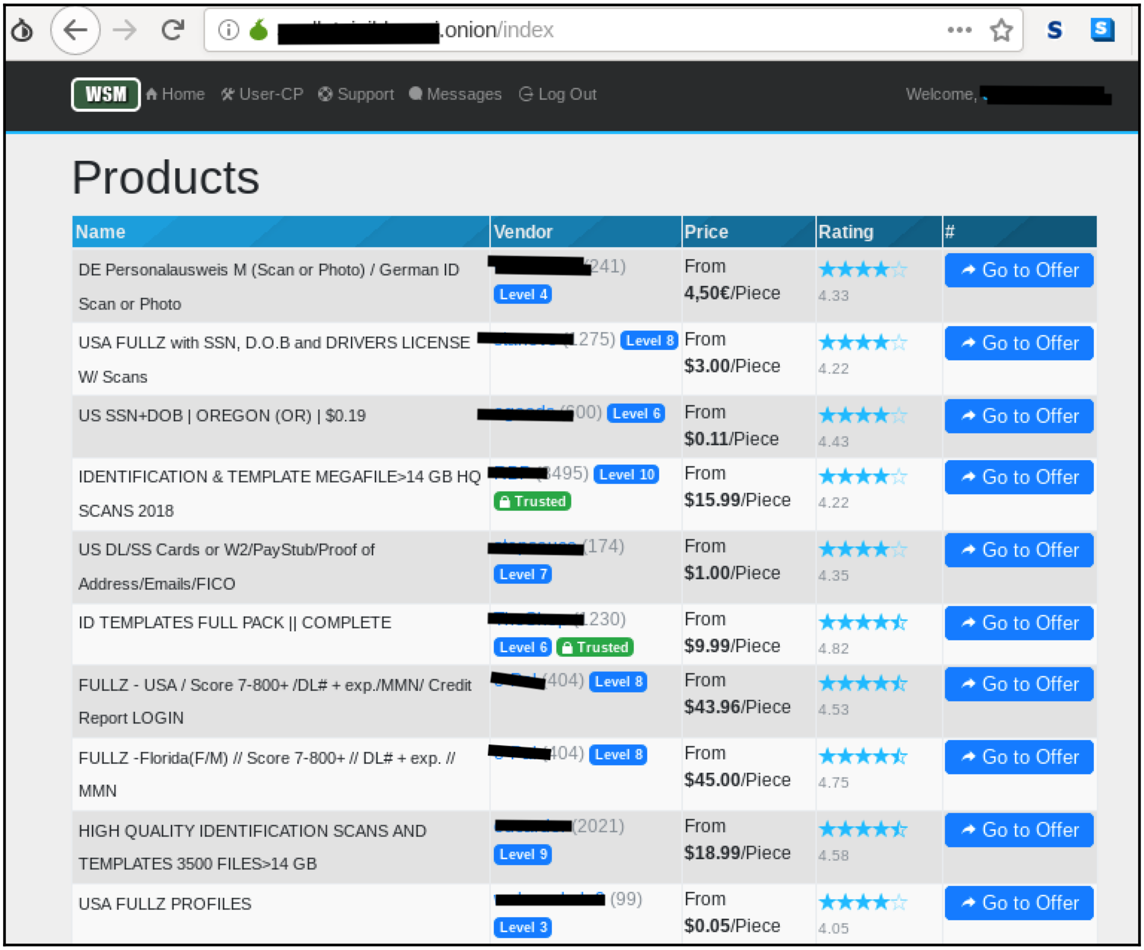
Search for..

- + Drugs 6113
- + Counterfeits 245
- + Jewelry & Gold 31
- + Carding Ware 51
- + Services 1090
- + Software & Malware 440
- + Security & Hosting 45
- + Fraud 1024
- + Digital goods 2572
- + Guides & Tutorials 2397

Wallstreet Market Categories

Counterfeit goods

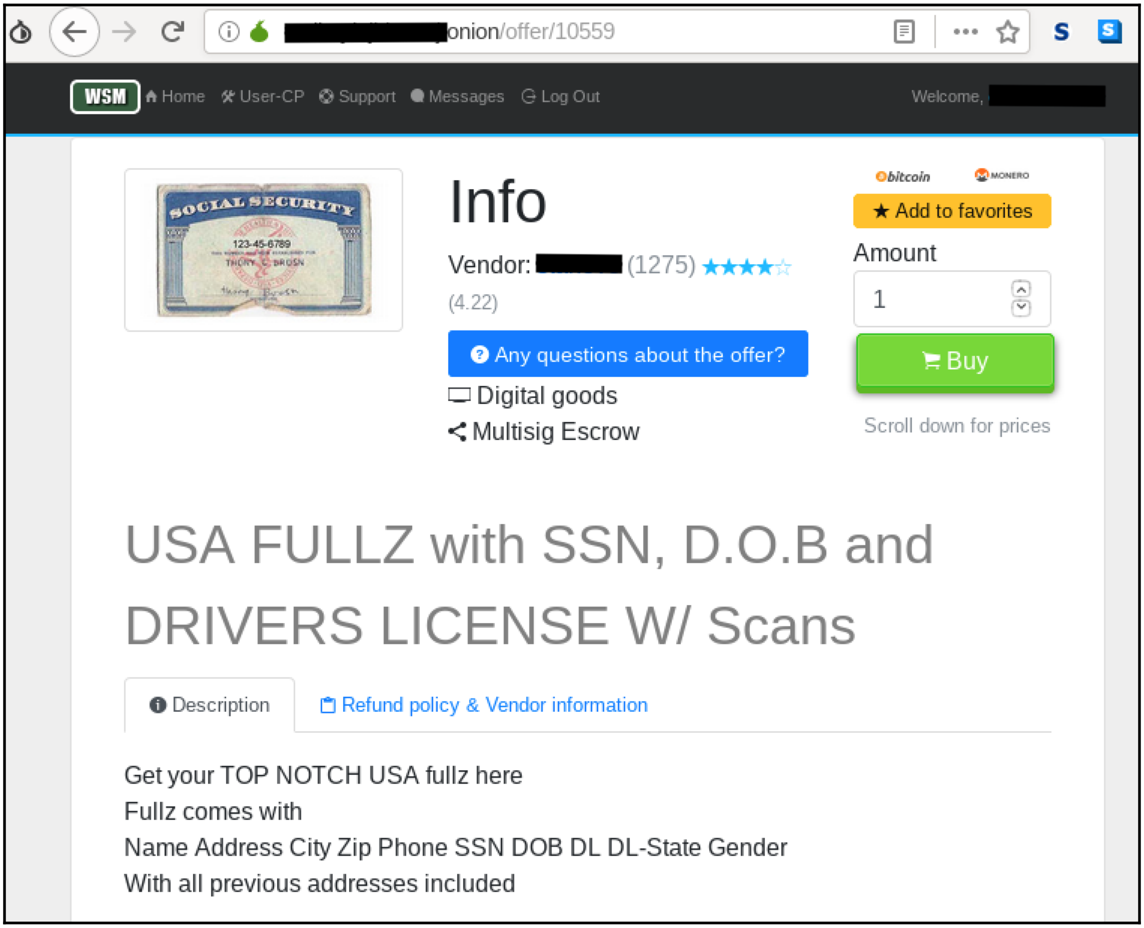
Within the Dark Web, you can find a wealth of counterfeit goods. These range from counterfeit electronics, currency, to even identification documents:



Products

Name	Vendor	Price	Rating	#
DE Personalausweis M (Scan or Photo) / German ID Scan or Photo	[redacted]241) Level 4	From 4,50€/Piece	★★★★☆ 4.33	Go to Offer
USA FULLZ with SSN, D.O.B and DRIVERS LICENSE W/ Scans	[redacted]275) Level 8	From $3.00/Piece	★★★★☆ 4.22	Go to Offer
US SSN+DOB | OREGON (OR) | $0.19	[redacted]00) Level 6	From $0.11/Piece	★★★★☆ 4.43	Go to Offer
IDENTIFICATION & TEMPLATE MEGAFILE>14 GB HQ SCANS 2018	[redacted]3495) Level 10 Trusted	From $15.99/Piece	★★★★☆ 4.22	Go to Offer
US DL/SS Cards or W2/PayStub/Proof of Address/Emails/FICO	[redacted](174) Level 7	From $1.00/Piece	★★★★☆ 4.35	Go to Offer
ID TEMPLATES FULL PACK || COMPLETE	[redacted]230) Level 6 Trusted	From $9.99/Piece	★★★★½ 4.82	Go to Offer
FULLZ - USA / Score 7-800+ /DL# + exp./MMN/ Credit Report LOGIN	[redacted]404) Level 8	From $43.96/Piece	★★★★½ 4.53	Go to Offer
FULLZ -Florida(F/M) // Score 7-800+ // DL# + exp. // MMN	[redacted]404) Level 8	From $45.00/Piece	★★★★½ 4.75	Go to Offer
HIGH QUALITY IDENTIFICATION SCANS AND TEMPLATES 3500 FILES>14 GB	[redacted](2021) Level 9	From $18.99/Piece	★★★★½ 4.58	Go to Offer
USA FULLZ PROFILES	[redacted] (99) Level 3	From $0.05/Piece	★★★★☆ 4.05	Go to Offer

The following is a screenshot of the counterfeit documents available online:



Info

Vendor: [redacted] (1275) ★★★★☆ (4.22)

USA FULLZ with SSN, D.O.B and DRIVERS LICENSE W/ Scans

Get your TOP NOTCH USA fullz here
Fullz comes with
Name Address City Zip Phone SSN DOB DL DL-State Gender
With all previous addresses included

Counterfeit USA identification documents

Stolen information

Many sites are hacked, their information stolen, and then dumped on the Dark Web either for free, or to be purchased by the highest bidder, or a specific customer.

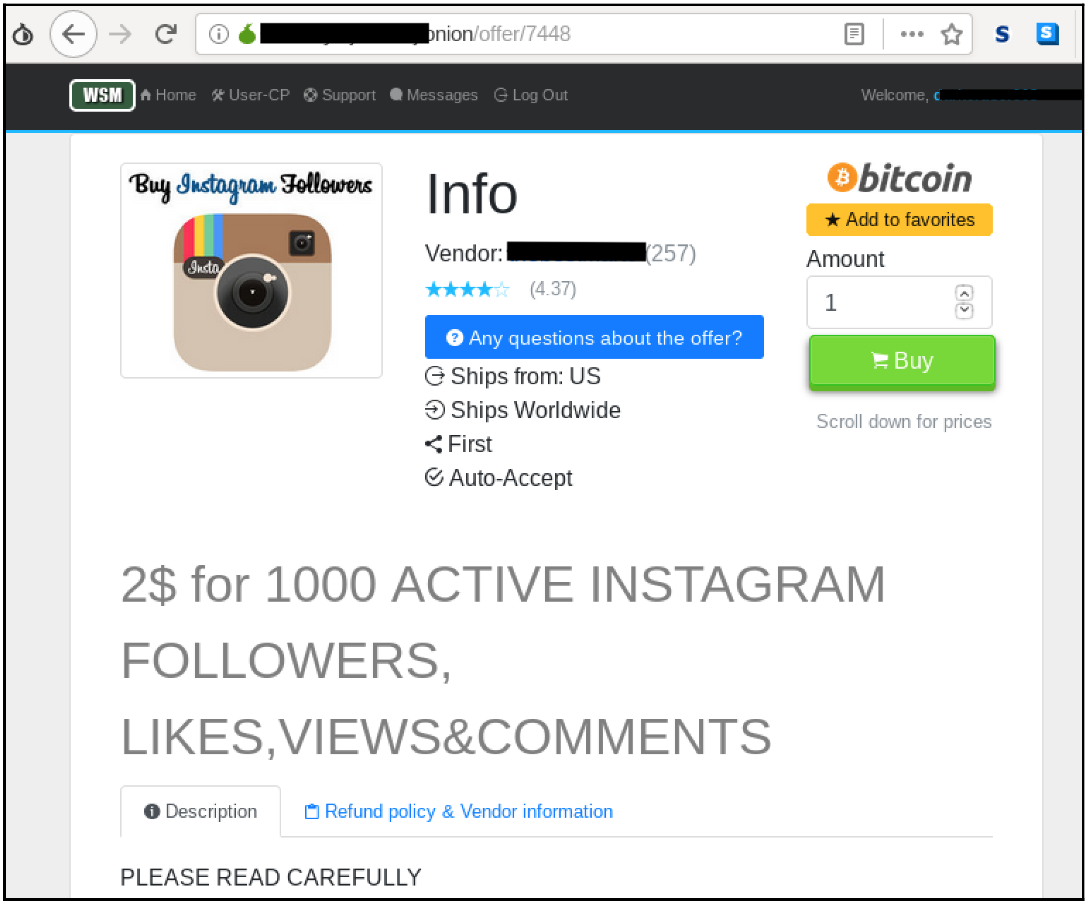
Today, there are many *dumps* of stolen data. Popular types of data are celebrity pictures, videos, and emails.

Hackers

In the past, hackers were considered dangerously highly-skilled professionals who should be kept at arm's length. Today, however, these individuals are sought after by enterprises, private companies, and nation states.

Black Hat Hackers are widespread on the Dark Web. These usually sell services, exploits, and tools on the Dark Web. They also use the Dark Web to communicate, plan attacks, and share exploits with each other.

Hacking services are very attractive on the Dark Web. Services offered by such hackers can be anything from performing a *realistic* penetration test to taking over a Facebook account. Such services are usually rendered at a cheap fee, which many can afford:



Info

Vendor: [redacted](257)

★★★★☆ (4.37)

Ships from: US

Ships Worldwide

First

Auto-Accept

Amount

1

Scroll down for prices

2$ for 1000 ACTIVE INSTAGRAM FOLLOWERS, LIKES,VIEWS&COMMENTS

PLEASE READ CAREFULLY

Hacking service to boost Instagram followers

The Dark Web holds a lot more than what was just described. There are sites that are dedicated to many beneficial or dangerous topics, such as hitmen for hire, killings, torture, and worse; or research, secure and anonymous communication, and more.

As you progress through this book, please be careful about how and what you access on the Dark Web, and do so at your own risk.

Read through the book before you go running to access the Dark Web, follow the explanations and recommendations, and always use Tor Browser, among other things.

Summary

In this chapter, we discussed what the internet is, what the Surface Web and the Deep Web are, what the Dark Web and darknets are, and observed several types of users of the Dark Web. We learned that in addition to being non-indexable, the Dark Web requires specialized software to access it.

In the following chapters, we'll discuss how to work with the Deep Web, and also discuss working with the Dark Web, a topic that we'll expand on as we go on in the book.

Questions

1. How would you label the three layers of the internet?

   A. Surface Web, Deep Web, internet

   B. Internet, Dark Net, Open Web

   C. Surface Web, Deep Web, Dark Web

   D. internet, Deep Web, Dark Net

2. What is responsible for indexing websites?

   A. Search engines

   B. Database servers

   C. Routers

   D. Bots

3. Organizations should exercise due diligence when storing privileged information on publicly accessible websites.

    A. True

    B. False

4. List three categories of data that are located on the deep web.

    A. Credit card information

    B. Private databases

    C. News headlines

    D. Academic journals

    E. Pictures hosted on Google Images

5. Name the components that make up the Dark Web.

    A. Darknets

    B. Firefox Incognito mode

    C. Overlay networks

    D. Content accessible using specialized software

6. Name two non-criminal uses of the Dark Web.

    A. Sale of counterfeit money

    B. Journalism

    C. Sale of an exploit tool you have developed

    D. Avoiding website tracking

7. Name two criminal uses of the Dark Web.

    A. Submitting a news article

    B. Obtaining a service to boost your Instagram followers

    C. Bypassing country censorships

    D. Buying counterfeit money

Further reading

The following resources might be interesting if you'd like to delve deeper into the topics included this chapter:

- `https://www.internetsociety.org/internet/history-internet/brief-history-internet`
- `https://www.history.com/news/who-invented-the-internet`
- `https://en.wikipedia.org/wiki/Deep_web`
- `https://en.wikipedia.org/wiki/Dark_web`