THE DARK WEB

Matt Beckstrom
Lewis & Clark Library
mbeckstrom@lclibrary.org
What is the dark web? When the Internet was created, the dark web did not exist. Basically, the Internet was an open platform with interconnected devices. Many of these devices were behind authentication walls, or other types of restricted access. Anything on the Internet that is not accessible from just regular browsing on the Internet is called in the deep web. Think of an iceburg. 90% of a floating iceburg is hidden beneath the surface of the water. The other 10% is visible. This is basically how the Internet works as well. The 10% showing is the surface web, and the 90% hidden is the deep web.

Examples of the deep web include any subscription database – most Facebook content, a lot of commercial sites, etc

In the early 2000’s, the Internet had grown to include so many people, and there were so many new ways to watch what people were doing, gather their information, etc and the Internet had become such an important communication tool, that some people felt the need to find ways to communication securely or anonymously. The dark web was born. Go back to the iceburg analogy. That 90% that is hidden beneath the surface? Take 10% of that and that is the dark web. Is it really 10%? That is unknown.
What is the dark web? When the Internet was created, the dark web did not exist. Basically, the Internet was an open platform with interconnected devices. Many of these devices were behind authentication walls, or other types of restricted access. Anything on the Internet that is not accessible from just regular browsing on the Internet is called in the deep web. Think of an iceberg. 90% of a floating iceberg is hidden beneath the surface of the water. The other 10% is visible. This is basically how the Internet works as well. The 10% showing is the surface web, and the 90% hidden is the deep web.

Examples of the deep web include any subscription database – most Facebook content, a lot of commercial sites, etc

In the early 2000’s, the Internet had grown to include so many people, and there were so many new ways to watch what people were doing, gather their information, etc and the Internet had become such an important communication tool, that some people felt the need to find ways to communicate securely or anonymously. The dark web was born. Go back to the iceberg analogy. That 90% that is hidden beneath the surface? Take 10% of that and that is the dark web. Is it really 10%? That is unknown.
What is the dark web? When the Internet was created, the dark web did not exist. Basically, the Internet was an open platform with interconnected devices. Many of these devices were behind authentication walls, or other types of restricted access. Anything on the Internet that is not accessible from just regular browsing on the Internet is called in the deep web. Think of an iceberg. 90% of a floating iceberg is hidden beneath the surface of the water. The other 10% is visible. This is basically how the Internet works as well. The 10% showing is the surface web, and the 90% hidden is the deep web.

Examples of the deep web include any subscription database – most Facebook content, a lot of commercial sites, etc

In the early 2000’s, the Internet had grown to include so many people, and there were so many new ways to watch what people were doing, gather their information, etc and the Internet had become such an important communication tool, that some people felt the need to find ways to communication securely or anonymously. The dark web was born. Go back to the iceberg analogy. That 90% that is hidden beneath the surface? Take 10% of that and that is the dark web. Is it really 10%? That is unknown.
The Internet started as a government way of communicating between facilities. The idea was to provide a way to facilitate instant communication and sharing information. Eventually, they allowed educational institutions to join. Using the same ideas that started with the Internet, other organizations formed their own internal networks. They eventually started connecting those separate networks together to form what we know as the Internet.

At first, the only security that people wanted or needed on the early ARPANET and Internet was the ability to prevent people from accessing what they should not. This was solved by isolating information away from the network, or by providing a login that needed to be provided.
When commercial sites started appearing on the Internet, they started finding ways to track user behavior. They wanted to understand how people use the Internet, what they shop for, and then serve them better ads. Much of this information was gathered without the permission of the user.

Governments started to track users to prevent crimes, and to prevent people from accessing information they felt to be against their views.

Due to the global nature of the Internet, it began to become a valuable communication tool. Many people, journalists and political dissidents needed ways to communicate that could not be intercepted.
The invisible Internet project was started in the early 2000’s as a way to provide anonymous communication on the Internet.

I2p is basically a layer on top of the Internet. It uses routers (i2p software installed on computers) that form ‘tunnels’. These tunnels are then used by other routers to send information around the layer until it reaches the end. It is a peer to peer network that uses various routers to communicate.

I2p is used for instant communication, websites (called eepsites), and other forms of communication. Mostly, it is used as an enclosed networks – the information you access is on the i2p network, but it can have exit sites that access normal websites.

To use the I2p, you install the software from the site. Once installed, you can use one of the tools designed to work on the network, or configure your computer to use it. Any program that uses a proxy configuration can be pushed into the I2p network.

Some tools that are designed to work with the network include I2P-messenger, a chat program, I2PSnart, iMule, file sharing applications, I2P bote an email program, and
many others.
The freenet project was created in the early 2000’s to provide a way to share files and communicate privately. It started as a research paper by Ian Clark in 1999.

Freenet is built similar to the way that the i2p is built – with nodes. Each device on the Freenet is a node, and traffic is passed between the nodes. The major difference is that the data on the I2P is stored on each device, but on the Freenet, information is stored all over the network on different nodes. The data is broken up, encrypted and then stored in different places. This gives users on the Freenet to store information without being connected. It also allows data to be stored in a way so that it is not linked to anyone person. It also allows the network to be scaled easily and have redundant storage.

Freenet is popular with anyone who wants to publish information or communicate in anonymous ways.

To use the network, you need to install the application, and then use an app that is designed to work on the network. Some examples include:

FMS – freenet messaging system
Frost – File sharing
Sone – discussions and images
TOR is probably one of the most familiar dark web projects. It was also started in the early 2000’s to provide a way to communicate anonymously. One of the biggest differences is that TOR is used to connect to the normal surface web in a way that is private. There are also websites stores on the TOR network (called .onion sites).

TOR uses a network of nodes to move information around. When a request is put on the network, it is routed to another node where it is encrypted and sent to another node. It keeps doing this until it reaches an exit node where it is decrypted and sent to the surface web.

You can use the TOR browser bundle to surf the .onion sites.
The dark net is not just used for crime. There is an element of illegal activities on the dark net. As with any anonymity service, people will use it for any purpose.

It is possible to purchase drugs or weapons on the dark web, but it also has a useful side.

The dark web is very useful for many other people

Dissidents in foreign countries – need the ability to get information out of their country
People in restricted countries - protection to access materials blocked by their country
Journalists – need ways to transmit information around the Internet
Information storage – anyone who needs to store information that may be considered risky
Regular people – who want to assure their privacy from surveillance
Yes! We are currently using TOR on the public computers at the Lewis & Clark library. Patrons who want to assure their privacy can use TOR any time.

The dark web can be used to educate patrons on Internet privacy.

Hosting dark web nodes assures that the networks are using reliable connections that are not being hosted by unreliable hosts or those who have bad intentions.
Of course, I have to push my new book. Me and another author Brady Lund are finishing up a new book called casting light on the dark web. It is due to be out by summer 2019 by LITA press.
QUESTIONS?