# Transcript: Tor Network and Browser w/ Michelle Williams

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker: Michelle Williams

WGU's IT audio series, flexible, portable, profound.

Michelle

Hello. Today we're going to talk about Tor. Basically, what is Tor? A little bit about the Tor network, the Tor browser. The Tor network is a popular free and open source software. It is on an encrypted network consisting of more than 6,000 relays and used to conceal a user's location. Tor's used by various different governments, students, researchers, and criminals. Tor is an acronym for the onion routing. Originally just termed onion routing, but then added that to it. That's where Tor came from. In 1995, onion routing was created by the Office of Naval Research that had a goal to, not specifically to provide anonymous communication, but just to separate identification from routing. In 2003, co-development was moved to the Tor Project and the Tor network was fully developed. Onion routing is a technique for anonymous communication over a computer network. In an onion network messages are encapsulated in layers of encryption, like layers of an onion. The end-user or initiator of a network traffic, encrypts traffic with multiple layers. A layer exists for each hop inside the Tor network. As the encrypted traffic moves through the Tor network, each node removes one layer of encryption, like removing a layer of an onion hence the name onion routing. At the last node, the final layer, the encryption is removed and the traffic proceeds out and onto the Internet.

Onion routing is the next layer of protection for when you don't want anyone stepping on your network to know what you're doing. They won't even know which server you are contacting and if you're even making requests or not making requests. So forensically, how do you deal with the Tor browser? The Tor browser is based on Mozilla's Firefox web browser and functions using onion routing. Browser provides access to dot onion websites available on the dot web. Tor's hidden service protocol allows users to host websites anonymously with dot bit domains which can only be accessed by the Tor network. How do you investigate malicious activities that were performed by using the Tor browser? The investigator should obtain memory dumps from the suspect's machine to extract the valuable information. Information such as websites browsed, emails accessed, etc. There are other artifacts that can be gathered as well on a Windows machine. One thing that they can do is run netstat-anl, and that will look for active connections.

Investigators can look for ports 9150 and 9151 for establishing connections via Tor nodes. User activity is also recorded in Windows registry. There are key specific to some Tor Browsers that they can look to identify and if a Tor browser is uninstalled or it's installed it in a different location than the default, it will be more difficult for investigators to know if a Tor browser was used or if it was installed, investigators will then have to go and examine the prefix file to obtain information that they're looking for.

As a forensic investigator, your main job is to see if the data is there or not there. To find this information, you might have to go hunt. You might have to research to see what other areas they might look for to find these files. There's other legal issues that come into play such as jurisdiction challenges or collecting this evidence from a Tor browser. The challenges that include our encrypted networks, the high level of anonymity, and legal jurisdictions all are issues when it comes to Tor browsers and Tor networks.

Those all come into play when looking into this particular Tor browser or Tor network.

Schedule time with your instructor to explore more deeply. WGU, a new kind of you.