INTERNET EVIDENCE

The Internet is a massive network connecting millions of computers together globally, forming a network in which any computer, smart phone or gaming device can communicate with any other computer as long as they are both connected to the Internet.

IP Address

Just as every house in a town has an address, every computer connected to the Internet has an address. This is referred to as an Internet Protocol (IP) address. Public IP addresses are assigned by Internet Service Providers (ISP). They can be dynamic or static:

- Dynamic addresses can change each time a user logs on to the internet
- Static addresses are permanently assigned

The IP addresses resolve to an ISP. The ISP tracks the IP address and maintains a record of the assignment of an IP address at any time.

Domain Name System

Websites use a Domain Name System (DNS) which is tied to an IP address. Domain Name System (DNS) servers are the "phonebooks" of the Internet. They maintain directories that match IP addresses with registered domains and resolve the text that people understand (the domain name) into a format that devices understand (the IP address). Domain names are registered with the Internet Corporation for Assigned Names and Numbers (ICANN)

Levels of the Internet

The internet is indexed by major search engines such as Google and Yahoo to make searching for websites and web pages fast and convenient. However, this "surface web" is just a small portion of what is available and the entire internet is not indexed and searchable:

Deep Web

Access to the deep web is available if you know the site address and may require user credentials such as an account and password to log in. This data is not available to the search engines so it is not indexed by the search engines.

Dark Web

The dark web usually requires a special browser such as TOR (The Onion Router) to access the content and often contains illegal information. Dark web content may be encrypted.

Peer-to-Peer P2P

Peer-to-peer networks are computer networks used to share files such as movie and music files. One of the first P2P networks was Napster which used a centralized server to share files with users on the network. Napster was shut down due to copyright infringement.

Today, there are still many P2P networks. Instead of a central server, the members' computers become the file servers. To be able to access the files on the P2P network, a user agrees to "share" files that they have downloaded. Because there is no centralized server, these P2P networks are difficult to shut down.

Tracking a User

When contraband files are shared via P2P file sharing, the computer sharing the file is identified via the IP (Internet Protocol) address of the computer. The IP address is tied to a service provider. The user is identified via subpoena by the service provider.

The U.S Department of Justice - National Institute of Justice (NIJ) has published a comprehensive Special Report titled ***Investigations Involving the Internet and Computer Networks***.

A copy of the complete publication is available in the Industry Standards/Best Practices section of the Digital Evidence Toolbox.

Wayback Machine

The Wayback Machine is a digital archive of websites and other information on the Internet. As websites change over time, the Wayback Machine periodically crawls web pages and saves them in digital form, indexed by date, for future review,

Preservation Considerations

When information is found during the informal discovery process, proper preservation is essential. Since it is easy to delete information from websites, it must to be preserved and stored as soon as it is discovered. In order to properly preserve internet evidence, it must be printed or stored electronically. Also, a date stamp must be included as well as proper documentation.

- It is dynamic and can change with usage.
- It can be maliciously and deliberately destroyed or altered.
- It can be altered due to improper handling and storage.

Time Sensitive

For these reasons, internet evidence is time sensitive and should be expeditiously retrieved and preserved. Also consider that when investigating offenses involving the Internet, time, date and time zone information may prove to be very important. Server and computer clocks may not be accurate or set to the local time zone. The investigator should seek other information to confirm the accuracy of time and date stamps.

Service Providers

Within the Digital Evidence Toolbox, Subpoena Guides section is the ***Cell-Social Media Subpoena Guide*** that outlines the contact information for popular service providers.

Conclusion

Rapid identification, assessment and preservation are the first steps in using internet evidence.

A defined set of best practices and industry standards exists governing the preservation and analysis of internet evidence.

Digital Evidence Toolbox - References

Subpoena Guides: ***Cell-Social Media Subpoena Guide***
Industry Standards/Best Practices: ***Investigations Involving the Internet and Computer Networks***

For more information on social media and internet evidence, call now and speak with a certified expert. I.R.I.S. LLC is available 24 hours in emergency cases.