What are some common ways you might discover services or applications that are helpful to an investigation?

Step 1:

Discussing the tools utilised by IT systems management and networking professionals is the fastest way to comprehend the data sources available for an investigation. They deploy systems for management, compliance, business continuity, and availability, and these tools collect and store a lot of data.

Step 2:

Determine the risk, what operating system to use, the hardware or software to use, the tools to use, and the security measures.

A few tools for digital forensics

Wireshark can be replaced with NetworkMiner, another Network Forensic Analysis Tool (NFAT), to extract or recover all files. Instead, Snort is a useful tool for locating network offenders in real time.

Are network services such as DHCP critical to incident response? If DHCP logs are not available, how might you still determine what system an IP address was assigned to?

Step 1:

A network protocol called Dynamic Host Configuration Protocol (DHCP) is used to set up network devices for IP network communication. A DHCP client obtains configuration data from a DHCP server via the DHCP protocol, such as an IP address, a default route, and one or more DNS server addresses.

Step 2:

Yes, the investigator receives crucial information from network services like DHCP. Examine other services that might reveal a relationship between an IP address and another property if DHCP logs are not kept. For instance, web proxy logs may link an address with a host name, and SAMBA logs may record the system and user identity.