Digital Forensics Process No matter which model is adopted, a few steps are common across all of them, such as:

Step 1: Investigation preparation: The first stage of any cyber forensic investigation. Here, investigators ensure they have the right tools and people. This ultimately depends on the type of event that is being investigated. In the case of a legal investigation, the investigation team obtains a search authority. In a criminal case, the search authority comes with a search warrant or a subpoena. In a civil case, it might just be consent to a search. Forensic tools are validated at this stage too. Investigators must clear each piece of hardware and software of issues and have their accuracy verified. This is especially important for new and old tools with new upgrades or patches. Sometimes, one may need a second round of validation before the analysis stage. Every time this validation is done, it needs to be documented. The processes mentioned above are crucial. If done incorrectly, it negates any findings from the investigation and cannot be used in court. In the case of incident response, external investigation teams require an SLA (service-level agreement), while internal teams just need to establish their chain of command. Once this is done, a list of possible digital devices and systems is created. This is done by looking for a digital footprint. The digital footprint traces an activity. For example, in the case of intellectual property theft, investigators look into the suspect's behavior on the system. This includes the applications they accessed, which websites they visited, and what devices were used. Tracing the digital footprint produces a list of assets. The items on this list are then seized for in-depth analysis, keeping the criminal intent in mind.

Step 2: Evidence identification: Once the initial details and legalities are determined, the second step is identifying the evidence and finding where it is stored. During this stage, it is essential to document the evidence, where it is stored, and the format in which it is stored. This could be an email or a video clip that indicates the event being investigated.

Step 3: Collection of evidence: The collection stage of digital forensics involves carefully extracting this evidence while ensuring no damage occurs. Sometimes, this step is as straightforward as making a hard disk copy and combing through it. However, it might not be as simple as it seems in all scenarios. This step can also involve recovering deleted files or cracking passwords to gain access. Data is also examined at this stage and whittled down where necessary. When the haystack is smaller, the needle is easier to find. Once the data becomes accessible, it is isolated and secured. Backups are created, making sure all content and metadata are the same.

Step 4: Evidence preservation: The original data that acts as digital evidence is now isolated and cannot be handled by anyone without authority. Forensic images are exact copies of digital proof, done at the bit level (0 or 1). The process of generating this bitstream image is called imaging. Hashing is a mathematical algorithm that processes the original bitstream and the images. The hashing function creates a unique value for every unique bitstream it processes. These hashes are treated as the 'fingerprints' of the digital evidence. An image and the original digital evidence are deemed the same if their fingerprints match. A chain of custody is established and documented during this stage. This chain of custody is crucial, especially if this evidence is to be used in court. It is a detailed account of the digital evidence, from when it was retrieved to when it is presented in court or to an auditing team. Each time evidence changes hands, it is noted next to a description of that piece of evidence at that point in time.

Step 5: Information analysis: All relevant digital data is examined during this stage, and the most relevant parts are analyzed and extracted. This relevant information is converted into a format one can use to present to the stakeholders or the court. The amount of time spent in this stage depends on the facts of the event. In some cases, it might stretch over a long period. It is essential to keep the circumstances and

facts of the investigation in mind. During the analysis stage, investigators try to establish a timeline, identify connections, locate illegal content, and determine whether a system has fallen victim to malware or any other form of cyber-attack. Once the analysis is complete, investigators form conclusions. An example would be marking 'likely' to a question such as 'Has this USB drive been tampered with?'. This step may take many iterations to reach a desired point of closure. Each action in this stage is documented in the interest of repeatability. Repeatability is required so that an authorized third party can reach the same conclusions by following the same steps with the same tools on the same piece of evidence. This establishes the authenticity of the investigation.

Step 6: Report presentation: Documentation is a step that runs alongside every stage of the digital forensic process. Once the investigation is completed, a post-investigation document covers all findings. The format of this document must be in line with the requirements of the court or client. Most forensic tools also auto-generate their reports to be consumed by experts. These reports are technical and cannot be understood by everyone. Most of these reports are not trial ready and must be adjusted to form a good presentation. The presentation of these reports varies based on the intended audience. For instance, in a court of law, the presentation must be simple enough for the judge and jury to understand while covering the steps taken to acquire the evidence. The presentation can make or break a case in someone's favor.