According to the Forensic Plan Guide, there are many steps for undergoing a network forensics investigation. It discusses the main phases of this process, as well as detailing how the investigation should be conducted to ensure there is no ambiguity in any aspect of the case. The phases detailed in the introduction are: the identification phase, preservation phase, data collection phase, examination phase, and reporting phase. All of these aspects are vital to the investigation, but some may change. The document specifies that the template for the phases mentioned above is not set in stone, and it may be altered to fit the specific needs of the investigation.

During the first phase, the identification phase, the the investigator must be contacted and informed of the current situation regarding the client's network infrastructure. This phase contains the Preliminary Investigation Discussion (PID) meeting. The PID is required to ensure that the investigator, client, and investigation team are all on the same page. The client will debrief the investigator on the incident in question, and if they have one, the Incident Response team will relay any vital information about the case to the investigator. This will likely include a topology of the network, an incident response plan, Point of Contact list, incident assessment, and the incident investigation report. Then, the computers and infrastructure that require investigation will be detailed. If the client has any additional questions or concerns, the PID would be the time to express them. Also during the PID, the investigator must estimate how much of the client's resources will be used. These resources can be anything from money, time, computing resources, and network resources. If the client decides that the cost will be too much, they may halt the investigation and close the case.

The investigator must also determine the legality of the investigation, by keeping in close contact with both the legal team and HR department of the client. Both of these departments will help protect the client and the investigator from litigation. The client must also specify the jurisdiction the investigator has. For instance, the investigator may be allowed to access a certain subnet of computers, but be restricted from accessing others. All of this would fall on the client to decide. In the event of escalation, the client and investigator must agree on the procedure for doing so. The PoC may not have a high enough level of access to the client's resources, and the investigator must work accordingly. During this phase, it's also important to keep a living timeline of the events that took place prior to the incident in question. This timeline should include known facts regarding the investigation, and they should be constantly revalidated to ensure robust accuracy of the report.

After the first phase, comes the planning phase. This phase is self explanatory, and describes how the investigator will proceed with the investigation. This is where the investigator should review their notes and scan for any inconsistent facts. Then, a risk assessment must be performed so that the client and the investigator know what problems may arise, and plan accordingly. If there is any possibility of disaster striking, the investigator will look for it in this phase. The investigator must also question what the suspect is capable of, and determine if they have any incentive/ability to destroy evidence. Once this has been completed, the investigator will conduct interviews to try to gather any other vital information from the teams. They will also need to determine what evidence will be collected, as well as how that data will be acquired. For instance, certain pieces of evidence will require different acquisition methods. Does the whole

drive need to be captured? Specific files? Will an exact clone of the drive be acquired or just portions of it? These questions should be answered long before the actual investigation commences.

During the preservation phase, the investigator must arrive at the scene, determine which computers are being investigated, and take photos of any useful evidence. This will include placing numbered photos tents on points of interest. It's also the investigator's responsibility to ensure that no evidence is tampered with. This may include putting tape over the computer's power plug, or adding crime scene tape to prevent unauthorized persons from accessing the area.

Then comes the data collection phase. This phase is where the physical and digital evidence bagged, tagged, and documented. Physical evidence can include anything from fingerprints to written down passwords or usernames. Once this evidence is collected, the scene can be processed for digital evidence. The machine's data must be imaged onsite to prevent any mistakes that may occur from doing so offsite. The machine should not be powered on prior to the image, as this may clear registers in the memory that are vital to the investigation. All backups should be acquired by the investigator and any drives containing collected data should be stored in anti-static bags to prevent data corruption, as it may destroy important evidence. The investigator should look at special content, email content, live acquisition, graphic images, documents, and any other files that may be important to the case. If child pornography is found, extra measures must be taken to protect the victim's identity and privacy. It can't hurt to periodically look through the evidence logs to ensure all evidence is accounted for and vet any evidence anomalies.

After the collection phase is the examination phase. To begin, the investigator must make certain that the forensic system used for analysis is wiped clean, so that no remnants of previous investigations tampers with the current evidence. Once the suspect's drive is collected, all partitions and unallocated space must be processed and documented. If there are multiple drives (such as a RAID configuration), it will most likely be up to the investigator's discretion on how to organize this data, as long as there is no written policy specifying how these drives should be organized. All disks have unallocated space that may contain important data that can be used as evidence. Experienced suspects will hide content in the slack space, so that it cannot be read by the normal OS. This phase would also be a good time to consolidate any evidence that might not be vital to the investigation, so the investigator has less to analyze and can save valuable time. It's also important to generate a file list with matching hashes to make sure these files aren't changed during the investigation. The investigator should create list of any files that have a changed file extension, as this may hint at the suspect trying to hide evidence.

The next phase of the investigation is analysis. The document specifies a few ways of analysis that will help the investigator form conclusions, such as temporal, relational, and functional. Temporal analysis is all about connecting the known events to the timeline with robust timestamps. Relational analysis is used to determine how digital evidence is connected to the ongoing investigation. Functional analysis is used to process how each piece of evidence functions within the investigation, and creating diagrams/descriptions of their importance. All three of these combined make up evidence analysis, which leads to a conclusion.

Finally, comes the presentation phase of the investigation. This is where the investigator will organize all documentation so far, write the report of everything that was accomplished, edit any final details that need polishing, and arriving at conclusions that will be shown to client.