Answer1.

1. When you are approaching the internet you must be careful about the fact that whatever is there in your own mobile and monitors it is going to be exposed to everyone, sooner or later. It's inevitable whether you are communicating either through mail or through secured WhatsApp, the data is going to be revealed to everyone. So the way you approach this device either your mobile phone or internet, you can consider it as an open broadcast medium and sooner or later, your photographs even if not communicated will be visible to the entire world.
2. The privacy level on the internet must be considered as the least. The smarter the device, the lesser be its security. You will feel that you are having end to end encryption in WhatsApp but the backup in WhatsApp is available for the people in the WhatsApp organization. It is important for us to understand that even though the e-mails we are writing are private, they are accessible to many people across the globe. The password we have set for our devices and accounts, it’s certain that you are not the only person to know the credentials.
3. It is important to understand that the trust factor is taken most clearly. Whatever you are putting on the internet is visible to everyone. So the words and the expression should be chosen in the most careful manner when expressed online. Our parents and elders told us not to trust anyone anonymous or unknown. It is more relevant in the world of the internet where we might not know the person behind the face behind that ID. Is it the actual person or not? So be cautious while using the internet primarily which has been seen time and again in the cases we study in cyber forensics.
4. When we know the limitations and reality of the Internet and devices, we will be careful enough and will have a more cautious approach while working on the internet. Being aware of the roadblocks we can make a decision more confidently and will be aware of the pitfalls and the scenarios. If we know where we can falter, this will give us a different sense of strength which ignorance does not. Hence knowing the limitation of knowing the fact about the internet will give us the freedom and the clarity using which we can take our decisions quicker and better.

***2.5 marks for each explanation. 8 marks for the above question in total.***

Ans2:

1. It’s Important for us to understand that while acquiring the data we must have the warrant for not only searching the place but also acquiring different evidence. Different lands have their own rules including Indian Territory, United States of America territory, Canadian territory and others. There is a special warrant that is required to search a place there is a separate warrant that is required to confiscate the devices. Which devices can be confiscated proper a justification needs to be presented to the magistrate.
2. The rules of the land clearly specify that we must make sure that the evidence confiscated matches with the evidence that has been treated. We found evidence is the same we are giving results. While we are getting any evidence we need to maintain the proper chain of custody and to maintain the hashcode. Also, prove it in the honourable Court of Justice that the evidence that we are presenting is on the same device that we have confiscated.
3. Laws of land give the right for any person to demand a proper thorough analysis of evidence. The vulnerability and the third party analysis right is provided to the accused. It depends upon the laws of the land which allowed the accused the right of full methodological analysis of the evidence. As forensic experts, we must be aware of it and careful that the evidence that we have collected can be used by the accused for further treatment and in-depth analysis.
4. As forensic experts, we need to understand that laws apply to a limited territory. For example, Indian law can be applied to Indian territory. They can not be applied on US territory. But cybercrime can take place in one Geographic region, can be performed from another Geographic region, and can execute through various other geographical regions of the land. E.g. The place where the crime has happened in Japan. The person who did the crime was sitting in Uganda and the communication that took place, for doing the cybercrime, was be routed through 10 different countries. We need to be careful of not only finding out the trail of evidence but at the same time finding out improving different laws of the land. How the accused can be prosecuted how the accused can be treated in which particular different geographical regions are different.

***ANY TWO of the above need to be discussed in-depth for fetching 8 marks in total.***

Ans 3:

1. We must have acquired the proper warrant from the magistrate not only for searching but also for confiscating the digital evidence that may be present. ***2 Marks***
2. It is important for us to make a copy of the hard disc that is used in the laptop. As the device is already running we keep track of and maintain the chain of custody.

For the applications that are currently running, we note it down and make a copy of the live instance of Random Access Memory. We keep track of what are the variables and the states of the applications that are running inside the machine. In order to maintain the proper chain of custody, we need to properly note down the evidence that has been confiscated also need to note down the hatches of the folders and files that will be used and the applications that are being treated for the evidence. We will look for the evidence for the places where it is at most important for search ***2 Marks***

1. The clues we need to search for the files that he may have used for hiding the files. the files hidden, store them as different one extension, make the partition hidden, accused can also use the software for hiding the particular files, he can make use of the slack space for hiding, he can delete the data, accused can use password-protected features for making sure that the device and the data are not accessible to us. We need to look for the various places, including the registry, into the deleted files, into the slack spaces, look for the mismatch headers. Search the files regarding the keywords specific to ATM number, etc. Look for browsing history for such searches. Searches for hardware devices and laptops/desktops need to be carried on persistently across the different mediums. The files specified in the places where the files will be hidden or deleted or corrected or concealed.  ***6 Marks***
2. We can use forensic tools like ftk, Encase, etc. We can also use hex editors for reading the headers and other places to note down the hash keys and mapping. We can also use password cracking software required We use write blockers, the tools that prevent any changes to be done on the hard disk. We also you to utilise the software that makes the disc to image copy. This can be done by forensic software like ftk, encase, sleuthkit (autopsy) etc. ***2 Marks***
3. In order to present the case properly. We maintain the chain of custody. We maintain that the evidence we are using is the same that was created for that we need to match. This needs to be provided properly in the documentation format. The places where the evidence was searched and how it maps to the particular person needs to be carefully presented to the lawyer. Who in turn will present it to the honourable Court of justice. ***2 Marks***