1. The purported offense entails the unapproved acquisition and dissemination of private images that are owned by Mr. Brendan Oliver. This falls under the categories of potential extortion or blackmail, illegal access to personal information, and invasion of digital privacy. Because of the nature of the crime, a comprehensive investigation is necessary to find the culprit, comprehend how the images were obtained, and stop such events in the future.
2. The following justifies computer forensic activities:

In this case, computer forensic operations are essential to: Find digital evidence of illegal access to Mr. Oliver's smartphone. Analyze communication routes to determine where the picture leak originated. Ascertain whether physical access, hacking, or some other method led to the breach. Establish a digital evidence chain of custody. Examine the gaps in Mr. Oliver's online safety. More details are required: a thorough account of what happened, who the images were emailed to, and any questionable behavior that Mr. Oliver or his team noticed.

1. Key Points for the Client:

* A methodical approach is taken to the investigation to ensure that no potential evidence is tampered with. We will examine gadgets, network logs, and communication channels using digital forensic tools. To piece together the exact timeline of the purported intrusion, investigators will create a timeline of events. The admissibility of evidence in court will be guaranteed by adhering to chain of custody regulations. Collaboration and regular communication with the client to exchange information, obtain updates, and obtain more data.

1. Sources of Information

* Smartphone: Mr. Oliver's smartphone will be forensically examined to look for malware or indications of illegal access.
* Email Accounts: Checking for possible leaks by looking through correspondence, particularly emails from months ago.
* Network log analysis: Look for any odd activity or unapproved access points in the network logs.
* Security camera footage: If accessible, use it to pinpoint the locations of physical entry points. To maintain the integrity of the evidence, forensic imaging involves taking pictures of pertinent gadgets.

1. Obtaining Acceptable Proof:

* Maintain the Chain of Custody: To guarantee the integrity of the evidence in court, properly record and safeguard all evidence.
* Obtain Legal Agreement: Make sure that all forensic operations abide by the rules and laws that apply.
* Adhere to recommended practices: To keep your reputation, use the computer forensics industry standard techniques.
* Record Everything: Keep detailed records of the investigation's methodology, conclusions, and any departures from accepted practices.

1. Potential queries and worries from the client:

* Who might be in charge of this breach and how did it occur?
* Is it possible to take the leaked photographs down from the internet permanently?
* What steps may be taken to stop privacy violations in the future?
* What is the expected duration of the research and what is the probability of success?
* What possible effects might this occurrence have on Mr. Oliver's standing?

1. Inquiries to Ascertain the Client's Next Steps:

* Could you give us a thorough rundown of everything that happened before the photo leak was discovered?
* Do you have any doubts or worries regarding certain people having access to the emailed photos or Mr. Oliver's phone?
* Has Mr. Oliver changed his digital security strategy recently?
* What details about the person to whom the images were emailed some months ago do you know?
* Exist any further instances or details that would be pertinent to the inquiry?

References

* Computer Forensics and Investigation: Nelson, B., Phillips, A., & Enfinger, F. (2019). "Guide to Computer Forensics and Investigations." Cengage Learning.
* Digital Forensics Best Practices: Casey, E. (2011). "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet." Academic Press.
* Privacy Laws and Cybersecurity: Solove, D. J., & Schwartz, P. M. (2015). "Privacy, Data Protection, and Cybersecurity in Europe." Aspen Publishers.