

Cyber Bullying and Harassment: Can Deleted Data be Recovered?

Timothy R. Primrose, Mobile Forensic Analyst

Bullying and harassment are often found to be easier to do online as opposed to in-person, not only because it is not face-to-face, but because it can be done anonymously. Social media platforms provide a space for users to develop an online persona consisting of photos, videos, opinions, life updates, and more. Users can engage with posted content with likes and comments, or can message “friends” directly. Social media and messaging data can be explored for cases involving cyber bullying, sexual harassment, and more.

Cyber Bullying Case Study

Background: A high school student received a handful of insulting messages on their Instagram account from a fellow classmate. In addition to the insults, a serious threat was made. The message receiver spoke with the school’s guidance counselor, which led to questioning the alleged sender about the messages. The alleged sender claimed that he did not send the messages and that someone else must have logged into his Instagram account.

Forensic Analysis: The alleged sender’s Instagram data provided evidence that allowed us to locate the real bully. The timestamps from the login activity for the sender’s Instagram account were compared to the timestamps of the messages sent from the receiver’s Instagram account. The device used to login to the sender’s account during these times was a Samsung Galaxy S8. The alleged sender owns a Google Pixel 6; however, that doesn’t mean he didn’t have two phones or the ability to login on a different device. The IP address associated with the logins relative to the messages was investigated and was traced to the home of another classmate. The classmate is friends with the alleged sender and owns a Samsung Galaxy S8. When questioned, the classmate admitted that he had previously watched the alleged sender sign into his account and memorized the password.

Sexual Harassment Case Study

Background: A woman conducted a virtual presentation for a couple dozen people in her office. After the presentation, she received a Microsoft Teams message from a colleague applauding her for her public speaking and oral abilities. The colleague then began to make obscene comments that made her feel very uncomfortable. She asked him to stop through the Microsoft Teams message service, which prompted him to delete all of his messages from the Microsoft Teams chat. The woman reported the event to the Human Resources (HR) department and was told there was nothing they could do since the messages were gone.

Forensic Analysis: DJS analysts received the colleague's work issued iPhone 12. By reviewing a SQLite database containing data relevant to Microsoft Teams, we were able to view the content of the deleted messages. The data was provided to the HR department for them to handle internally.

With the influx of people learning and working from home, teachers and managers are not present to monitor the safety of students and office staff, leaving them more susceptible to cyber bullying and harassment. DJS can help answer the questions of who and why in these situations by collecting data from social media and messaging platforms.

Timothy R. Primrose, Mobile Forensic Analyst with DJS Associates, Inc., can be reached via email at experts@forensicDJS.com or via phone at 215-659-2010.