

# [Criminal analysis and mapping](https://assignbuster.com/criminal-analysis-mapping/)

[](https://assignbuster.com/)[Law](https://assignbuster.com/essay-subjects/law/)

Criminal Analysis & Mapping College Chapter exercise Education experience Data analysis studies form the main part of crime education for most crime analysts. Social science studies in quantitative analysis are a major ingredient in this field.   
Previous related work experience   
The analyst police and investigation work background are useful in this field. The statistic experience is also quite useful in this field.   
Analysis responsibilities   
Sharing pertinent information with law enforcement officers provides analytical assistance for investigators, prepare crime information, review and analyze tendencies and patterns, develop tactics to prevent future crimes and provide reports on criminal activities within assigned area.   
Overall impression   
It is an involving and interesting profession. It requires multi skills and good interpersonal skills. A crime analyst works within a team hence the need for team work skills. It is a challenging, dynamic and ever evolving field with a high demand and commitment from the individual.   
History of crime analysis and crime mapping   
Crime mapping is used by analysts in law enforcement agencies to chart, envision, and explore crime occurrence patterns. It is a key element of crime analysis together with other policing tactics. Mapping crime, permit offense analysts to spot crime spots, alongside other trends. Therefore crime analysis is a supportive component in crime analysis.   
Chapter 2 exercise 1   
1. Motive to commit crime   
Out of curiosity and need to challenge security systems on online platforms. The friend was always keen to find out confidential information from unsuspecting online accounts.   
2. It was in a quiet cyber café tacked in a secure neighborhood.   
3. The target was virtual accounts that have links to credit card payment systems. The target was on active online accounts which would be difficult to detect hacking attempts.   
4. Failure by owners to heed to calls to change security information regularly, weak passwords and failure to use secure procedures when logging into their accounts (Williams, 2007).   
5. Using secure sites and methods of online payments, changing security information to evade tracks and limits amounts and period for transactions. Heavier penalties for cyber crimes would deter potential offenders.   
  
References   
Williams, G. (2007). Online business security systems. New York: Springer.