Psychological Profiling and Computer Forensics: Locard’s Principle in the Digital World
Dr. Marcus K. Rogers & Kate Seigfried (CPT Cyber Forensics Lab)

Abstract
The current project examines the need to extend psychological crime scene analysis from its current supportive role in physical crime scene analysis, to an identical role in digital and cyber crime scenes. The fundamentals of crime scene analysis are discussed and a focus on the ability of psychological cyber crime scene analysis to answer the FBI’s critical elements is presented. A model illustrating the analogous physical and cyber crime scene elements is provided. The importance of cyber victimology in profiling and target hardening is also briefly examined, as is the importance of not being fearful of the seeming uniqueness of computer crime scenes. Finally, suggestions for future study are offered.

Locard’s Principle of Exchange
“When a person commits a crime something is left behind at the scene of the crime that was not present when the person arrived.”

Crime Scene Phases
1. Recognition – knowing what to look for, what constitutes potential evidence, and more importantly what can be ignored. This phase also includes the collection of the evidence.
2. Identification – once evidence or potential evidence has been recognized, it needs to be identified. Identification consists of classifications at the most basic level based on class characteristics (e.g., hair, blood, fingerprint). This allows for identification to be analogous in both worlds.
3. Comparison – the collected and identified evidence needs to be compared to some standard or control to determine that it came from a particular class (e.g., paint from a 1975 Ford Mustang).
4. Individualization – the evidence is then further examined to determine any unique characteristics that would allow it to be differentiated from the larger category to a specific person, or entity/object based on its unique characteristics (e.g., paint from a 1975 Ford Mustang owned by the primary suspect).
5. Reconstruction – the last phase ties together the previous phases and allows the investigator to pull together the pieces of what has been to this point part of the puzzle with no real picture to follow, into a logical sequence of events consistent with established timelines.

Crime Scene Elements
1. Victim selection
2. Victim characteristics
3. MO of the offender
4. Attitude of the offender towards the victim
5. Offender’s reaction to victim’s behavior
6. Offender’s language
7. Violence used by the offender
8. State victim was left in
9. Forensic evidence left at the scene

Future Research
Future research needs to extend the work that has been done in re-purposing traditional investigative support disciplines to the non-traditional cyber world. Specifically, future studies should attempt to validate the crime elements mapping approach (see Table 1) to ensure that the proper analogous conventional and cyber elements are identified. Researchers should use some type of factor analysis to determine the minimum set of elements necessary to provide the most utility to investigators across various cases (e.g., virus attackers, insider fraud, intellectual property theft, identity theft). The area of cyber-victimology also requires more concentrated attention, especially with regards to the development of a victim typology.

“When you have eliminated all which is impossible, then whatever remains, however improbable, must be the truth.”