The Digital Forensics Cyber Exchange Principle

Adapted from Forensic Magazine online,
by Ken Zatyko and Dr. John Bay (2011)
(http://www.forensicmag.com/articles/2011/12/digital-forensics-cyber-exchange-principle#.UmhAH1Ooh9k)

Locard's Principle of Exchange is a trusted idea in the field of forensic science that states that "With contact between two items, there will be an exchange." This means that – it is believed – that no person can commit a crime without leaving *some* trace of evidence behind. This principle has become the most central concept of crime scene investigation. Its application to cyber crime (crimes committed online or with the use of sophisticated computer-based technologies) brings a new and exciting dimension to the famous Locard exchange principle.

"…This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study it, and understand it, can diminish its value."
(Kirk, 1953)

"Artifacts of electronic activity in digital devices are detectable through forensic examination, although such examination might require access to computer and network resources involving expanded scope that may involve more than one venue and geolocation."
(Zatyko and Bay, 2011)

Locard's Exchange Principle is named for Dr. Edmond Locard (1877–1966) who was a pioneer in forensic science. He was known as "the Sherlock Holmes of France." He formulated the basic principle of forensic science: "Every contact leaves a trace." Granted Locard probably never envisioned the computer wherein a laser comes in contact with magnetic media to flip bits. Fragmentary or trace evidence is any type of material left at or taken from a crime scene, or the result of contact between two surfaces, such as shoes and the floor covering, or fibers from where someone sat on an upholstered chair.

When a crime is committed, fragmentary (or trace) evidence needs to be collected from the scene. A team of specialized police technicians go to the scene of the crime and seal it off. They record video and take photographs of the crime scene, the victim (if there is one), and any physical evidence. If necessary, they undertake a firearms and ballistics examination. They check for shoe and tire mark impressions, examine any vehicles, and check for fingerprints.

For the digital crimes of today, specialists need to examine a much more complex environment. Investigators need to image digital media of a multitude of types: magnetic, solid-state, or optical, for example. Evidence might be persistent, such as that stored in non-volatile memories, or fleeting, such as over a transmission medium that has no storage. Evidence might also exist in media that is volatile but only temporarily accessible, such as DRAM on a live system or "weakly" erased disk data. Furthermore, the investigation may involve more than the subject and host machine. It could also involve routers, servers, backup storage devices, and even printers, just to name a few.

A crime scene is the location where an illegal act took place. In cases involving digital media, the geo-location of these scenes could be thousands of miles away because of networking devices such as routers, switches, servers, internet exchange points, and policies related to traffic management by internet service providers.

In this article we present a challenging question for today's digital forensic experts, cyber scientists, and cyber analysts: Does Locard's Exchange Principle – developed in a world that had no digital technologies – apply in digital forensics? The dramatic increase in cyber crime and the repeated cyber intrusions into critical infrastructure demonstrate the need for improved security. The Executive Office of the President noted on May 12, 2011, "Cyber threat is one of the most serious economic and national security challenges we face as a nation."[2] We believe addressing whether or not Locard's Exchange Principle applies to digital forensics is a fundamental question that can guide or limit the scientific search for digital evidence.

Locard's Exchange Principle is often cited in forensics publications stating that "every contact leaves a trace…" Essentially Locard's Exchange Principle is applied to crime scenes in which the perpetrator(s) of a crime comes into contact with the scene. The perpetrator(s) will both bring something into the scene, and leave with something from the scene. In the cyber world, the perpetrator may or may not come in physical contact with the crime scene, thus, this brings a new facet to crime scene analysis.

The field of digital forensics can be strictly defined as "the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation."[3] Furthermore, digital evidence is defined as information stored or transmitted in binary form that may be relied on in court.[4] However, digital forensics tools and techniques have also been used by cyber analysts and researchers to conduct media analysis, compile damage assessments, build timelines, and determine attribution.

According to the Department of Defense Cyber Crime Center's training program, cyber analysts require knowledge on how network intrusions occur, how various logs are created, what is electronic evidence, how electronic artifacts are forensically gathered, and the ability to analyze data to produce comprehensive reports and link analysis charts.

Our hypothesis is that Locard's Exchange Principle does apply to cyber crimes involving computer networks, such as identity theft, electronic bank fraud, or denial of service attacks, even if the perpetrator does not physically come in contact with the crime scene. Although the perpetrator may make virtual contact with the crime scene through the use of a proxy machine, we believe he will still "leave a trace" and digital evidence will exist.

Breaking the exchange principle into its parts and analyzing its application, one has to determine whether or not the following occurs:

- Are there two items?
- Is there contact?
- Is there an exchange of material?

To illustrate the application of Locard's Exchange Principle to a cyber crime, we take the example of identity theft where someone's identity is stolen and the perpetrator intends to use the stolen information for criminal gain. Let us further suppose the perpetrator steals the identity through the use of a Trojan horse virus and keyboard logger on the victim's computer. One could contend that during this type of cyber crime Locard's Exchange Principle does not apply. The rationale is that because a human is not at the crime scene there is no trace evidence from the human on the computer or digital media at the scene. However, in actuality there may be lots of digital evidence such as the Trojan horse itself, changed passwords, digital logs, and so on. Thus, in this example, there is a trace at, to, and from, the scene. It may involve finding the trace evidence at other physical locations than just the one scene of the crime. The keyboard logger could be added software or hardware or both, but in both cases it remains behind for an investigator to discover.

From our perspective, Locard's Exchange Principle does apply to this example. However, we may want to generalize it into the "Cyber Exchange Principle" with the following caveat:

> Artifacts of electronic activity in conventional digital computers are detectable through forensic examination, although such examination might require access to computer and network resources beyond the bounds of the "crime scene" itself.

Electronic contact does not leave a physical trace because a human or thing does not come in contact with the scene. It may leave only digital evidence and therefore extensive examination of evidence beyond the primary physical crime scene (the location where a law was actually violated) should occur. This examination typically involves bits and bytes of information.

For example, if an unauthorized user gains access to an unsecured system to exfiltrate information to a remote site, he will, on the surface, leave no direct evidence because no files were altered. However, if file access logs were maintained, a record will be made of the file access and subsequent network transmission. Even if no log files are kept, a side-channel analysis of disk activity, system calls, and network operations may be available as evidence. Failing that, network logs at the ISP (internet service provider) level might provide evidence related to the unauthorized access, even if the exfiltrated data itself cannot be identified.

This proposed Cyber Exchange Principle addendum brings a new and exciting dimension to the famous Locard Exchange Principle. As stated earlier, we believe Locard's Exchange Principle can be used as the foundation for digital forensics much as it is used for traditional forensics. However, we challenge the reader to prove us wrong. Do instances exist in cyber crime where Locard's Exchange Principle does not apply? If such examples do exist then these instances need to be analyzed, fully described, and accounted for in the development of cyber systems. For example, if a crime is described where Locard's Exchange Principle does not apply, this could lead to new sensors or methods to supplement current cyber security systems. On the other hand, if no examples are given that disprove Locard's Exchange Principle in a digital crime then we can use the principle as a foundational guidance in digital crimes, as forensic examiners have done for years in the physical world.

We illustrate our hypothesis with two examples. The first example has a direct counterpart in the physical world—an electronic bank robbery wherein money is stolen from one account and fraudulently sent electronically to another. In this example an illegal electronic transaction occurred. There was no human trace at the scene (no shoe prints on the floor, no fingerprints on the keyboards). Instead, just bits across a network processed by computers. There may be log files of the transactions, passwords that were changed, money transferred between accounts, and so on. This is the indirect (non-physical) evidence which must be analyzed. This evidence could be temporary, volatile, semi-permanent, or permanent. Timeliness of evidence seizure may be critical. Since there may be no contact by the perpetrator at the bank, there is no trace evidence from the human perpetrator at the physical scene of the crime. This is exactly why venue becomes an important decision point with prosecutors handling computer crimes. It is true there is trace evidence by the perpetrator at the originating computer. It is also true that through the use of proxies at interim hop points the perpetrator never had to come in contact with the scene of the crime.

The second example involves a botnet investigation. In this example the perpetrator may or may not take things from the scene. In fact, the motive may be to deny service of a system or systems to legitimate users (such as in the recent forced shutdown of PayPal by angry WikiLeaks supporters). The perpetrator in this example is known as a bot master and secretly infects thousands of computers with copies of a computer program known as a "bot" (short for robot, but, in this case, completely digital). A bot can have legitimate functions, but can also be used to gain unauthorized access to and control over computers that they infect and can thus cause the infected computers to attack other computers. Bots used for such illicit purposes are frequently disguised as MP3 music files or photographs that unsuspecting computer users download from public Internet sites. Having downloaded an infected file, a computer user is usually unaware of the presence of a bot on his or her computer. Focusing solely on the injected malicious software code may not lead to attribution because it could have been borrowed or stolen and not written by the perpetrator(s). It may only be an instrument of the crime. If the code was designed to automatically vary itself, it may not match what is currently on the perpetrator's computer. This makes timeline analysis even more critical.

However, we contend that digital evidence exists in this instance. For example, if bots are used to spam a legitimate site causing the site to slow down or become non-functional, there will exist transactions between the bots and the legitimate site. In fact, the bots themselves are digital evidence. While capturing and analyzing the digital evidence may not be easy or even possible today, the fact that evidence exists supports our hypothesis that Locard's Exchange Principle does apply.

More research is required in the cyber domain, especially in cloud computing, to identify and categorize the unique aspects of where and how digital evidence can be found. End points such as mobile devices add complexity to this domain. Trace evidence can be found on servers, switches, routers, cell phones, and other devices. At least in the two examples described above, digital evidence can be found at the expansive scenes of the crime which includes numerous computers as well as peripheral devices. It is now time to look beyond the primary, physical "crime scene" for digital evidence. Investigators must expand their search to include the entire computing network. Many times, the computer crime investigator must explore several scenes to find the evidence. To aid in this quest, digital forensics standards are required now more than ever.

References

1. Kirk, P. L. (1953). Crime investigation: Physical Evidence and the Police Laboratory. New York: Interscience Publishers.
2. Lew, Jacob, Memorandum to the Speaker of the House of Representatives, May 12, 2011, www.whitehouse.gov, last viewed June 16, 2011.
3. Zatyko, K. (2007). Defining Digital Forensics, Forensic Magazine.
4. National Institute of Justice (2004), Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Washington, DC.
5. Galiardi, P. and Leary R. (2011), Making Sense of Evidence, Forensic Magazine.
6. Lerner, K. Lee and Lerner, Brenda W. (2005) World of Forensic Science, Volume 2.