Executive Summary

The collection and analysis of network traffic is extremely useful to the Forensics Investigator (FI). Unfortunately, this is an involved process that requires a high level of expertise in networking where a good deal of the useful information requires a low level analysis of network protocols. Furthermore, many of the UNIX based tools require that the user be proficient in this environment. Still much of the information encapsulated in live network traffic is such that it can not be found elsewhere.

Note: The text book [1] does an excellent job introducing the reader to the topic of Network Forensics (Chapter 8 & 14). Therefore, the goal of this paper is not to repeat that material but to supplement it.

Digital Forensics Purpose

Network Forensics or Network-Centric Forensics, as defined by Tao Security, “finds compromised systems, intruder activity, and incident scope.” [2] Network forensics is often associated with Network Intrusion Detection (NID) because many of the same tools and techniques that have been developed for NID are used in Network Forensics. The main distinction, made by Richard Bejtlich, is that NID is alert-centric whereas network forensics requires a network-centric approach. [3] Network-Centric Forensics collects Network-Based Evidence (NBE) [4] with the intent of providing the investigator initial clues for further analysis. Because NID is an alert-based approach the assumption is that a set of predetermined criteria can be used to detect malicious activity. NID is not necessarily concerned with NBE beyond raising an alert. One reason that Network-Centric Forensics requires a more dynamic and in-depth analysis than NID is because it concerned with collecting evidence or exposing indications of the source of an incident.

In the book The Tao of Network Security Monitoring: Beyond Intrusion Detection, Richard Bejtlich defines Network Security Monitoring (NSM) as “the collection, analysis and escalation of indication and warnings to detect and respond to intrusions” [5]. Because of the FI requirement for evidence, a NSM strategy is a more suitable tactic for network forensics than a NID approach. Local or state law enforcement, federal agents and network administrator are just a few of the different roles that a FI might take on. Though each of these roles has different motivations and restriction, all require the
collection of presentable evidence. It is usually not enough to know that an incident happened; often documented details and sources are needed. It is not that NID can not be extended to achieve these goals but that this is not necessarily the intent of NID.

Is network traffic really that useful to a forensic investigator? In many ways network traffic is one of the more reliable sources of digital forensic evidence. For instance, if a compromised computer is analyzed and if the perpetrator was a highly skilled, the forensics investigator might be outwitted and never uncovering any useful evidence. But if that same computer is monitored on the network and if that computer is being actively used for malicious activities there will be NBE. It might be obscured using a covert channel or encryption; still there will be a trail of evidence in the form of network traffic. [2] This means that NBE is an extremely useful form of digital evidence.

State of Practice

Traffic Collection

One aspect of Network Forensics is that the information is momentary. If network traffic is not captured while it is being transmitted it is gone. Granted the effects of the traffic might still be evident, and there is certain to be clues of a network related event, still this is not nearly as useful as live network traffic. One of the consequences of this is that timely decisions are required to be made about whether to collect network traffic or yank a suspected machine off of the network. Often this decision might be made for the investigator based on warrants or company policy. If it possible to obtain, live network traffic will often be an extremely useful source of information. It can confirm or refute suspicions and often will uncover other possible sources of evidence.

The textbook [1] defines three types of network monitoring event monitoring, trap-and-trace monitoring, and full-content monitoring. Full-content monitoring will be the focus of this paper since this is the most useful. Collecting live network traffic will empower the investigator to determine a plethora of information. The following are some of the items that could be determined from live network traffic:

- Protocols and port numbers that are running on particular computers. It should raise flags in the investigators mind if for instance a network printer is running acting as an FTP server.
- The Operating System (OS) of particular computers. This can often be determined because certain OS have particular signatures and often use proprietary protocols.
- What computers are communicating with what other computers? If the network file server is initiating a connection to another country the file server might have been comprised.
- The volume of network traffic from a particular computer. If a computer is a member of a Botnet and is actively being used in a Distributed Denial of Service
(DDoS) attack there will be a large amount of similar traffic originating from that computer.

- What attachments are sent over the network can be determine and even captured. See the open source tool TCPExtract. This could be useful if it is it is suspected that a computer is being used to transferring trade secrets over the network.
- If the communication protocol is clear text the actual contents of the message can often be determined. This information might include email messages, user name, passwords, etc..
- Other suspicious behavior can often be identified. For instance if a covert channel is being used then there will be signs of abnormal protocol usage like strange use of TCP flags. Encrypted communication using a port that is typically use by a protocol that doesn’t use encrypton would be suspicious.

How does one go about collecting network traffic? The answer largely depends on the network, the role of the investigator and the nature of the incident. There are some general guidelines that should be observed. First and foremost the collection machine should not be detectable on the network. There are instances in which a network administrator might use probing techniques that introduce specially crafted packets in order to illicit a response. But the FI does not want the collection device to introduce any traffic onto the target network. The ideal is that the collection device be completely transparent on the network and undetectable by all other devices on the network.

There are various ways to have an undetectable collection device. Which way is chosen largely depends on the equipment available, the configuration of the target network, how much traffic needs to be collected, as well what type of traffic needs to be collected. One way to keep a computer from producing network traffic is using the network configuration utilities on the collection device. Depending on the OS of the collection device the techniques and effectiveness of this will vary. A sure way to keep the collection device from introducing packets on the network is to sever the lines used for transmission on the network cable used. This might seem odd and severe but it seems to be common practice as is outlined here [4] and here [6]. Another secure method is to buy or construct a tap interface [7]. This is a device that has a network port that is wired to only receive and not transmit data. Most tap devices that you can buy have an internal buffer that will buffer traffic during bursts of network activity, thus lessening the likelihood of the collection device dropping packets. Similarly, some switches have a SPAN port that is designed specifically for collecting network traffic [8].

Another consideration when setting up the collection device is the logical location. The collection device needs to be strategically placed on the network so that it can see the traffic of the targeted device(s). This can be complicated by a switched network. In a switched network traffic generally only gets sent to the physical port in which a machine with that address resides on. Thus, simply placing the monitoring computer on the same network as the target device will not ensure that the monitoring device will see any of the traffic of the target device. This is an instance where a SPAN port is very convenient.
I will not go into detail about how to get a computer to capture traffic that is not addressed to that device. The tools mentioned below can be used for this and often have tutorials describing how to use them. Unfortunately, most of these tools require a higher level of knowledge about network protocols than I would expect most law enforcement to have. Additionally, many of these tools require that the user be skilled with the OS that they run on. This is probably not an issue for most system or network administrator but I would guess that most local and federal law enforcement investigators probably don’t have this level of proficiency in this area. Thus, the area of Network Forensics tends to be a specialized area requiring a focused skill set.

**Wireless Network Traffic**

I will not try to explore all of the special considerations in regard to wireless, but a simple illustration should serve useful. Generally all that is required to see traffic on a wireless network if to be within a particular proximity of an access point. Unlike wired networks where one needs to physically plug a wire into a network device. This has a dramatic effect on network security. For the FI this means that an incident on the network need not be confined to the computers in that building. An attack could come from a perpetrator in a car across the street. Thus the ease and level of anonymity is dramatically higher than on a wired network. There are certainly many effective ways to secure a wireless network but the most significant vulnerabilities will likely come from a rouge wireless access point under someone’s desk and not the infrastructure set up by the system administrators. Thus, a wireless survey of the area can often be very insightful. For an in-depth coverage of the topic I recommend *Wi-Foo: The Secrets of Wireless Hacking* – Vladimirov, et all.

**Network Forensic Tools**

Network Forensics seems to be an immature field in which most of the tools have been borrowed from NID or other network monitoring tools. Below is a list of some of the more useful or common open source tools used for Network Forensics:

- **Ethereal** is a GUI application (Tetheral is the text based counterpart) used for gathering and analyzing network traffic. This tool is an extremely useful tool that does protocol analysis using descriptors and color highlighting. Ethereal has the ability to extract TCP sessions and group them in sequential order. This tool can analyze traffic in multiple formats. Note: Recently this project has been changed to Wireshark. [http://www.ethereal.com](http://www.ethereal.com), [http://www.wireshark.org](http://www.wireshark.org)

- **TCPDump** – is very efficient and a powerful tool for collecting network traffic allowing for the use of filters so that a subset of network traffic can be captured. This is very handy if the investigator who is restricted by a warrant and is required to only capture traffic from a particular machine or network. [http://www.tcpdump.org](http://www.tcpdump.org)
- **Snort** – is an extremely customizable open source NID tool that can be used to collect traffic. Because of its flexibility it is easily integrated into other tools. [http://www.snort.org](http://www.snort.org)

- **Sguil** – is a client/server based application where snort is the main source of information. Sguil allows the investigator to quickly analyze various levels of network traffic is a customizable GUI. [http://sguil.sourceforge.net](http://sguil.sourceforge.net)

- **TCPExtract** – is a tool that will capture file attachments that are traversing the network. [http://tcpxtract.sourceforge.net](http://tcpxtract.sourceforge.net)

- **TCPFlow** – is a network capture and analysis tool that can reconstruct TCP sessions. [http://www.circlemud.org/~jelson/software/tcpflow](http://www.circlemud.org/~jelson/software/tcpflow)

- **LiveCD’s** – Many LiveCD’s are useful for both network forensics as well as general Digital Forensics. This site lists and categorizes most of the LiveCD’s available. [http://www.frozentech.com/content/livecd.php](http://www.frozentech.com/content/livecd.php)

- **Netcat** – Dubbed as the TCP/IP Swiss army knife this simple yet powerful tool can be used to transfer data over the network in a raw form. It is used extensively by people on both sides of the law (e.g. many backdoor programs use Netcat). [http://www.openbsd.org/cgi-bin/man.cgi?query=nc](http://www.openbsd.org/cgi-bin/man.cgi?query=nc), [http://netcat.sourceforge.net](http://netcat.sourceforge.net)

- **Ngrep** – is an attempt to port the functionality of the grep utility for use with network traffic. [http://www.packetfactory.net/projects/ngrep](http://www.packetfactory.net/projects/ngrep)

- **Kismet** – is a very powerful wireless network sniffer that can be used to enumerate all of the local access points. [http://www.kismetwireless.net](http://www.kismetwireless.net)

- **Other Useful Links:**
  - [http://sectools.org](http://sectools.org)

As mentioned before, most of the tools used in Network Forensics are either the same as those used in NID or some variation of them. Because the ways in which network communication rapidly changes most of the tools used to collect network traffic function at a low level, this is not to say that they are not powerful they are as well very flexible. The area that seems to be lacking is in tools that aid in analysis.

---

**Works Cited**

[1] Incident Response and Computer Forensics – Mandia, et.al)