

PROFITAP

BUILDING A PORTABLE NETWORK FORENSICS KIT



VISIT WWW.PROFITAP.COM



WHY A PORTABLE KIT FOR NETWORK FORENSICS?

Network forensics and cybersecurity teams need to have the ability to intercept network traffic, and capture data packets in real-time to prevent threats and live attacks. Corporate organizations need to set up the network-interception and traffic-capture mechanism according to the size and architecture of their network. For example, companies with large networks with distributed data centers have to deploy multiple capture points, feeding to a central packet analysis appliance (network analyzer) that would be able to receive and analyze data at 10 Gbps or even up to 100 Gbps.

Unfortunately, not all companies have multiple data centers in a distributed architecture. In fact, most small-to-medium organizations have their entire IT infrastructure hosted at a single site. Most of these companies are not in a position to invest heavily in costly network security analysis products. It can be said that top management prefers to spend their budget on IT production equipment, rather than on IT support equipment, especially expensive network analyzers which can lead to security breaches.

Small-to-medium enterprises can benefit from a portable network forensics kit. At a much lower cost, it still enables you to perform real-time forensic analysis on any segment of your network on an on-demand basis. Not even large multi-branch organizations cannot deny its usability and benefit.

Imagine a cyber attack case in which a branch gets disconnected from the head office, and the local IT team wants to conduct a forensic analysis on their branch's internal network. Or, what if the network analyzer appliance gets isolated within a data center due to an issue in the internal connectivity? For situations like these, a portable forensics kit would be highly valued by the IT support team, given the short investigation window, even in case of large enterprises.

The beauty of a portable network forensics kit lies in its portability, allowing a quick deployment to any field location and instantly plug it on any network segment, without needing a dedicated power source.

BUILDING A PORTABLE NETWORK FORENSICS KIT

You can build a portable kit for forensics analysis with the following three essential tools.

A LAPTOP

The first thing you need is a laptop. While this sounds obvious, you must make sure you have the right laptop ready for a network forensics job. Here are the minimum specifications: 4GB of RAM, a fast storage device (SSD) with a capacity of at least 500GB, a 1Gbps network card, a USB 3.0 port, and a battery backup of 3 hours. Most modern laptops today already come with those specs. While most laptops come with an HDD, we highly recommend an SSD (Solid State Drive) based storage since they are much faster than HDDs, and speed is what you need for proper capture. Before you begin to perform forensic analysis on your network, you would first need to capture and store packets on your laptop.

Having SSD storage would give you a significant time advantage if you can store and parse the packets as quickly as possible during a security crisis. Compared to an HDD, which has a maximum disk-write speed of typical 100 MB/s, an SSD writes to disk much faster at 500 MB/s or more (even more for some SSDs). This is critical because you would need to have at least 250 MB/sec of disk-write speed, as we will explain in the next section.

A key point to remember is that this laptop should not be a common machine under routine use by the IT team, as that would mean lots of applications installed on it, with significant registry changes and memory load, resulting in slower performance. Rather, this laptop should be a specific machine dedicated for special purposes, such as forensics analysis or field troubleshooting.

The requirement of having a USB 3.0 port will be explained in the next section.



A PACKET ANALYZER

Next, you need a packet analyzer (also known as a packet sniffer), which is a tool (software or hardware) that can log, parse, and analyze traffic passing through a network. As data flows over the network, the packet analyzer receives the captured data packets and decodes the packet's raw data, revealing the values of various fields in the packet (e.g. TCP header, Session details, etc). You can analyze these values according to the appropriate RFC specifications to deduce whether the packet sustained any abnormal behavior during its transportation between the network points.

There are also various open-source packet analyzers available, among them Wireshark is the most popular solution. While its functionality is similar to the "tcpdump" tool, the best part is that it has a GUI front-end with integrated filtering options which are really useful to sort through the packets in less time. Also, it's free. More details of how to benefit from this feature are described in the next section.

A PORTABLE NETWORK TAP

In order to pursue network forensics, you need to have a specific device for packet capture that intercepts and captures packets from live traffic. Out of the two ways to capture packets, port mirroring (SPAN) and network TAP, the latter is more reliable, and accurate. A TAP has the power to capture packets on the wire, guaranteeing 100% of packets capture from live traffic in real-time. TAPs are being used extensively in security applications because they are non-intrusive and are undetectable on the network, having no physical or logical address. Thus, the forensics team can execute their activity in an invisible mode.

Amongst the various types of TAPs available today, portable TAPs are fast gaining popularity due to the flexibility to carry them in the field and deploy them instantly, at any location. They can easily be connected to your laptop, and with a tool like Wireshark installed, your laptop turns into a portable kit ready to commit to any troubleshooting or forensic task at hand.

Most manufacturers have their own variety of portable TAP's. However, not all of them are as good as they sound. Some of them are powerful yet difficult to handle without being truly portable. Some of them are easy to deploy but not powerful enough to fully capture the traffic. A portable TAP that is powerful enough to take on the full traffic, and yet easy and fast to deploy on the field, is the perfect tool for you.



BUILDING A PORTABLE NETWORK FORENSICS KIT


Forensic analysis is specialized work that requires years of expertise. Like a seasoned medical physician that diagnoses the illness by quickly reading the symptoms, a forensic analyst needs to be able to quickly detect anomalies in the network by looking for the right symptoms. This, of course, comes with years of practice. However, there are a few basic steps that you can start your forensic analysis from. Here is a quick list of clues that you should look out for during your forensic analysis.

CHECK EVENT TIMING

Event timings, i.e. time between events, are critical to identify whether there is malicious activity going on in your network. Events rolling out in short time spans, say a few hundred milliseconds or even a few seconds, is an indicator that these events are being generated by bots or malware, and not by a human. The range of these short time spans, milliseconds to seconds, depends on the nature of activity which a network administrator should generally have an idea about. For example, receiving dozens of DNS requests for a single website from the same source IP within few milliseconds, or receiving several DNS requests for a single website from multiple source IPs within few milliseconds, are some examples indicating that these requests could be generated from automated scripts initiated by bots or malware.

CHECK DNS TRAFFIC

Since DNS is the primary handler of all requests going out to the internet, you should check for traffic activity of your DNS server. If there is a rogue system, or a network worm in your network that is interested in making outbound connections to the internet, then you could detect its malicious activities on the DNS server. As mentioned earlier, one of the key edges Wireshark has over other analyzers is the option to filter packets by protocols or IP address. Using this feature, you are able to filter all packets for your DNS server's IP address, and check for requests received by your DNS server in specific time windows. If you see an unusually high number of connection requests in a short time span, say a few hundred milliseconds, from the same source IP, then you should suspect this is malicious activity and dig deeper into the packet headers to investigate further.



In case your DNS server is being bombarded with a very high number of requests, chances are that it is under a DoS attack (see more details ahead).

CHECK FOR MAN-IN-THE-MIDDLE ATTACKS

This is one of the most common attacks executed in an organization's network. Man-in-the-Middle (MitM) attacks are those in which an attacker tries to penetrate into the network by acting as one of the trusted systems within that network. In an MitM attack a rogue system intervenes between two trusted systems, and hijacks their conversation channel to divert all traffic through itself. The two trusted systems believe they are communicating directly with each other, whereas in reality they are communicating via the rogue system. This allows the rogue system to not only listen to the entire conversation but can also modify the conversation. The most common method to execute an MitM attack is through ARP spoofing, also known as ARP cache poisoning. In this technique, the attacker broadcasts false ARP messages in a LAN to associate its MAC address with the IP address of a trusted system in the LAN, e.g. the default gateway, the DNS server or the DHCP server, depending on the attack plan.

Using the filter option, filter all the packets to view only ARP packets. If you see a large quantity of ARP traffic (broadcasts and replies) then this is something suspicious. Because in a running network where all trusted systems usually have the MAC-to-IP mapping in their cache, you should not see a long list of ARP messages. Dig into the source and destination addresses in the packet headers and investigate further to find out if a MitM attack is taking place.

CHECK FOR DOS (DDOS) ATTACKS

This is also one of the most common attacks, conducted either internally within a network or externally from outside the network. The aim of a DoS (Denial of Service) attack is to make the resources of a machine or network become so consumed, that it eventually becomes unavailable to its actual users. DoS attacks are commonly made on Web servers to suspend the web services as the server is connected to the internet. In a DoS attack the rogue system bombards the target server with TCP/

SYN messages requesting to open a connection, but the source address is either a false or forged one. If the source is false, the server is unable to respond with the TCP/SYN-ACK message since it is unable to resolve the MAC address of the source. If the source is forged, the server responds with a TCP/SYN-ACK message and waits for the final ACK message to complete the TCP connection. But since the real source never initiated this connection, the server never received the final response and keeps waiting with a half-open connection. In either case the server is 'flooded' with TCP/SYN requests resulting in an unusually high number of incomplete connections, therefore saturating the number of connections a server can possibly make.

To quickly identify if a DoS attack is happening, filter to view TCP packets in Wireshark. Use the the option on Wireshark for viewing the packet-sequence graph which illustrates the flow of TCP connections with arrows between source and destination systems. If you see a large number of TCP/SYN packets being bombarded from a single source IP to the destination server IP, and either no reply back from the server IP or only the SYN-ACK message but no ACK reply from the source, then you are most probably viewing a DoS attack live in action.

In case you see a long stream of TCP/SYN requests being bombarded from multiple source IP's to a destination server IP, then this is a DDoS (Distributed Denial of Service) attack in which multiple rogue systems attack a target server, and is more lethal than a DoS attack.



THE BEST PORTABLE TAP FOR YOUR NETWORK FORENSICS KIT

You need a portable network TAP that does not create any bottlenecks or issues as described in the previous page. A TAP that is truly portable, should be pocket-sized, easily connected to a laptop, and yet powerful enough to fully capture 100% of the traffic, without any loss of packets or lag in packet-timing.

ProfiShark 1G is the world's best, fastest and truly portable network TAP for packet capture in any field location. ProfiShark 1G is pocket-sized and power-packed. It works as a packet capture tool without the bottlenecks of any packet drop or time delay. With the 2 x Gigabit network ports, it flawlessly combines the two traffic streams to transport over a single monitoring port. It does not use a Gigabit NIC as the monitoring port. Instead, it utilizes the power of USB 3.0, which can transfer data at up to 5 Gbps. Hence it can easily transport 2 Gbps of aggregated traffic stream (1G from each direction) over a USB 3.0 link.

This means that the buffer memory doesn't need to drop any packets and does not have to store packets long enough to impact their timing. Because it can easily connect to your laptop's USB port, the best part of the plug-&-play ProfiShark 1G is that it is not dependent on an external power source. Combined with a laptop, you have a truly portable and powerful packet capture & analysis kit, ready to use at any location without depending on a power source.

ProfiShark 1G can capture and transfer packets directly to your laptop at full line-rate – 2Gbps – provided you have SSD in your laptop, as we recommended in the previous pages. (In order to capture and store packets at full-line rate of

2Gbps, a disk-write speed of 250 MB/sec is required. All packets are captured in real-time, with nanosecond time-stamping at hardware level on each packet as it enters the TAP. This allows real-time analysis of captured traffic with nanosecond resolution.

The ProfiShark 1G comes with its own GUI-based configuration software, the ProfiShark Manager, which works in parallel with any network analyzer (Wireshark, Omnicap, etc.) and is compatible with both Windows and Linux platforms. You can configure the ProfiShark 1G using the various features shown on the GUI.

One of the benefits of the ProfiShark Manager is that it also allows traffic capture directly on your laptop in 1-click, without particularly needing a network analyzer to capture the traffic. This is especially helpful in situations where you need to capture traffic on a remote network segment and want to analyze it on a different computer other than your laptop, by exporting the PCAP file. The GUI also has a Counters section which displays the internal counters for both network ports, A and B. This shows the number of valid/invalid packets, CRC errors, collisions, and different packet sizes. It's a quick way to see the quality of traffic being received on each port without having to open a network analyzer.





DISCOVER PROFISHARK



Go to: www.profitap.com/profishark ▶

Go to: www.profitap.com/profishark ▶

IT ALL STARTS
WITH VISIBILITY

PROFITAP

Profitap develops and manufactures hardware and software solutions that help you get complete access and visibility into your network. These network visibility solutions are designed with the security, forensics, deep packet capture and network & application performance monitoring sectors in mind.

Profitap network solutions help eliminate network downtime, add security to existing and new networks all over the world, assist in lawful interception applications and reduce network complexity. All of Profitap's network monitoring tools are highly performant, secure and user-friendly, and provide complete visibility and access to your network, 24/7.

As we are experts in our field, we have developed our products set new standards in an industry where the definition of excellence is constantly being challenged.

With more than 1,000 clients from 55 countries, Profitap has become a must-have solution or many important businesses, many of which are among Fortune 500 companies.

**PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS**

sales@profitap.com
www.profitap.com



Profitap



@Profitap



profitap-international