Flowmon Packet Investigator (FPI) is an automated network traffic auditing tool that records and interprets full packet data.

Where flow data is not sufficient, and more detail is needed, the Investigator captures all the packets of traffic surrounding the event for in-depth troubleshooting.

What sets the Investigator apart, is built-in expert knowledge. It not only provides extensive details but automates the analysis, assessing the captured events, looking for error codes, and providing explanations and suggestions for a remedy.

### EXAMPLES WHERE FPI CAN HELP

<table>
<thead>
<tr>
<th>Network connectivity-related issues</th>
<th>Malfunction or misconfiguration</th>
<th>Client/server encryption incompatibility</th>
<th>Application protocol stack issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication blocked by the firewall, destination unreachable, TCP errors, etc.</td>
<td>Of critical network services such as ARP, DNS, DHCP</td>
<td>SSL/TLS version, encryption algorithms, certificates, etc.</td>
<td>HTTP, SAMBA, FTP, IMAP, POP, etc.</td>
</tr>
</tbody>
</table>

90% of MTTR is spent trying to figure out that there is indeed a problem.

35% of network management time is spent on reactive troubleshooting.

Source: Zeus Kerravala, ZK Research

Source: Network Management Megatrends 2018, EMA
Intelligent Decision-Tree Analysis

The Investigator digests PCAP files, which can be imported or recorded upon event detection, alert or custom trigger. It processes them using an analytical engine to locate the root-cause of operational issues and suggests remedial actions.

Investigation

The PCAPs are automatically analyzed for deviations from the RFC specifications of the respective protocols and their combinations, and any error codes or other failures are recorded. The list of currently supported protocols includes all of the most common services used by enterprises, such as TCP, IP, HTTP/S, IMAP, SMTP, DNS, DHCP, SMB, and many more.

In-built expertise

The Investigator draws on databases of error codes and translates them into a clear message. For example, when a client attempts to negotiate an encryption channel with the server but, due to certificate mismatch, the communication fails.

Instant knowledge

The results are presented on a dashboard showing the number of issues and their severity, allowing the user to immediately focus on relevant errors and act without delay.

Flowmon’s team of networking experts with decades of combined experience in the field are constantly working to expand the built-in expertise with interpretations of error codes and suggestions for remedial actions.
**FPI vs. Wireshark**

Wireshark is the most popular packet analyzer out there. It is available as open-source and is used by millions of users.

Unlike Wireshark, the FPI uses sensors distributed over the network, allowing packet capture to be triggered remotely and at any time and dedicated network sensors allow support of up to 100G speeds. Instead of manual analysis, it uses an analytical engine to process the packets and automatically displays any issues found. While expert users possess the knowledge to learn all they need using Wireshark, it may be difficult and time-consuming to use for less experienced admins. This is where the FPI comes to its own - it supplies the expertise and automates the labor.

**Recording**

On-demand capture is a powerful tool that stores relevant packets, even at 100G speeds, instead of capturing everything and consuming resources unnecessarily.

A variety of capturing triggers is available, from planned triggers based on a set of rules like MAC address, IP address, subnet (CIDR), protocol, port, VLAN tag, or MPLS label to manual or fully automated triggers.

**Automated trigger**

Consider this example: Flowmon ADS detects an Indicator of Compromise where a device is trying to access a domain known for malware distribution. This event triggers packet capture and thus ensures that full packet data is available for thorough analysis.

**Rolling buffer**

The rolling buffer allows a set of packets per flow to remain buffered for a defined period and recorded on-demand. This approach is a lightweight alternative to continuous packet capture that ensures that no packets are lost.