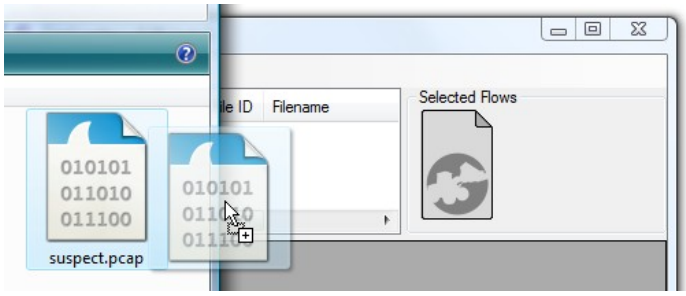
CapLoader

Overview of Functionality

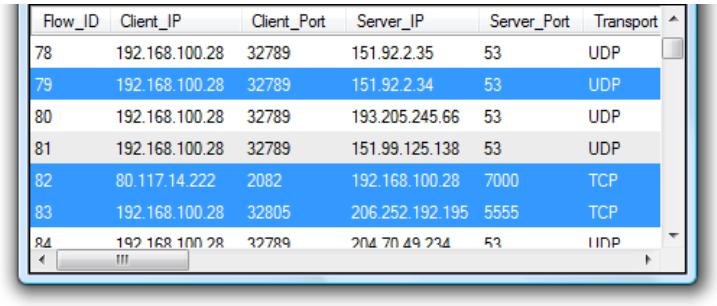
CapLoader is designed to handle large amounts of captured network traffic in libpcap (PCAP) and PcapNG format. CapLoader displays the contents of opened capture files as a list of TCP and UDP flows. Users can select the flows of interest and quickly filter out those packets from the loaded capture files. Opening the selected flows/packets in a packet analyzer tool like Wireshark or NetworkMiner is then just a mouse click away.

The typical process of working with CapLoader is:

1. Open one or multiple pcap files, typically by drag-and-dropping them onto the CapLoader GUI.

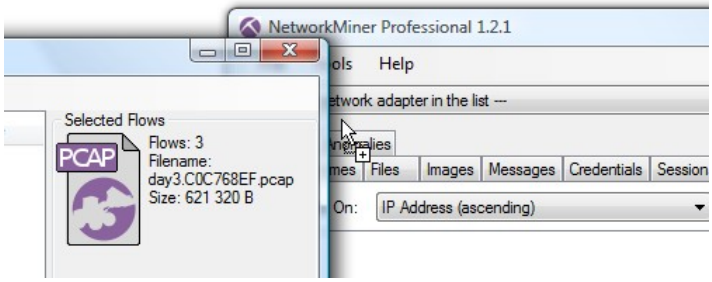


2. Select/mark the flows of interest.



Flow_ID	Client_IP	Client_Port	Server_IP	Server_Port	Transport
78	192.168.100.28	32789	151.92.2.35	53	UDP
79	192.168.100.28	32789	151.92.2.34	53	UDP
80	192.168.100.28	32789	193.205.245.66	53	UDP
81	192.168.100.28	32789	151.99.125.138	53	UDP
82	80.117.14.222	2082	192.168.100.28	7000	TCP
83	192.168.100.28	32805	206.252.192.195	5555	TCP
84	192.168.100.28	32789	204.70.49.234	53	UDP

3. Double click the PCAP-icon to open the selected sessions in your default pcap parser (typically Wireshark) or better yet, do drag-and-drop from the PCAP-icon to any application you wish.



Loading Capture Files

Capture files can be loaded by selecting “File > Load” from the menu, but a better way to do it is to select one or multiple pcap files in a directory and then drag-and-drop them onto CapLoader. You can also drop a whole folder onto CapLoader in order to load all PCAP files contained in the folder.

Capture files can be loaded directly from a web or FTP server by doing “File > Open URL”. It is also possible to open a capture file from an URL simply by drag-and-dropping a link to a capture file onto CapLoader, but your luck may vary depending on which web browser you're using.

The capture file formats supported by CapLoader is currently libpcap (.pcap), pcap-ng (.pcapng) as well as Gzip (.gz) compressed capture files.

Selecting Flows of Interest

Selecting flows (a.k.a TCP or UDP sessions) in CapLoader works just as you expect it to; flows are selected by clicking them with the mouse, holding [*shift*] allows selection of a range of flows and pressing [*ctrl*] allows additional individual flows to be selected or un-selected. Right-clicking a flow causes a context menu to display the option of selecting all other flows with the same IP or port numbers.

The “Hosts” tab provides an easy way to select all flows for one (or several) IP addresses. Selecting a host will cause CapLoader to filter out all flows to and from the selected IP.

Flows can also be selected based on log entries from an IDS[1], firewall log[2] or flow tool[3] by clicking “Edit > Select from Log”. Individual log entries can be loaded by pasting them into the flow selection form. It is also possible to load a whole log file by drag-and-dropping it onto the flow selection form.

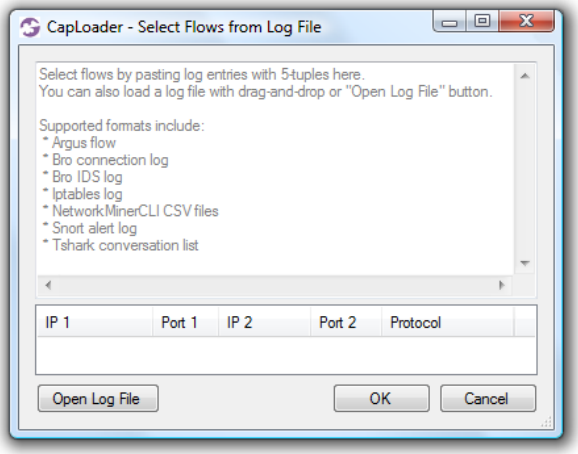


Illustration 1: Select flows from log file

1 Supported formats include Snort alert log and Bro IDS log

2 Supported formats include iptables format

3 Supported formats include Argus output, Bro connection logs and tshark conversation lists

Opening Selected Flows

Selecting one or multiple flows causes CapLoader to filter out the individual packets (frames) for these flows and making them available for export as a new capture file. The PCAP icon in the top-right of the GUI can be used to open the filtered frames in any of the following ways:

Illustration 2: PCAP icon

- Double-click the PCAP icon to open the frames with the default PCAP viewer (typically Wireshark).
- Drag-and-drop from the PCAP icon to any Packet analyzer of your choice (we recommend NetworkMiner).
- Drag-and-drop the PCAP icon to a folder to export the capture file to disk.
- Right-click the PCAP icon and select a tool to open the capture file with.

Transcript

CapLoader has the ability to show a transcript of the application layer data in a UDP or TCP flow, much like Wireshark's "Follow TCP Stream". Simply right-click a flow and select "Flow Transcript" to bring up a Transcript window.

The application layer data presented in the transcript view is shown exactly the same way the packets were captured. This means that data in retransmitted packets will appear twice and data in out-of-order packets will appear out-of-order.

The Transcript window also contains a PCAP icon, which can be used to extract all the frames associated with the flow being transcribed.

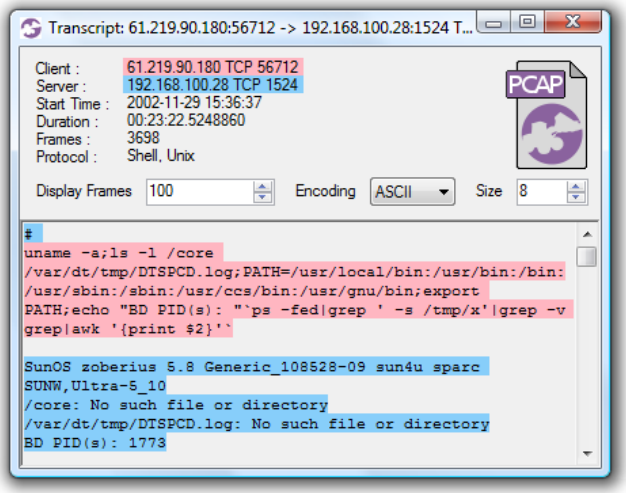


Illustration 3: Flow Transcript Window

Protocol Identification

CapLoader includes the ability to identify protocols without relying on port numbers[4]. This feature can be enabled by checking the “Identify protocols” check-box in the GUI. Loading capture files with the “identify protocols” feature enabled will cause the application layer protocols of the extracted flows to be identified and displayed in the flow list. Being able to identify the application layer protocol is important in order to detect what services that run on non-standard ports as well as to detect if common ports[5] are being used to transport other protocols than what might be expected.

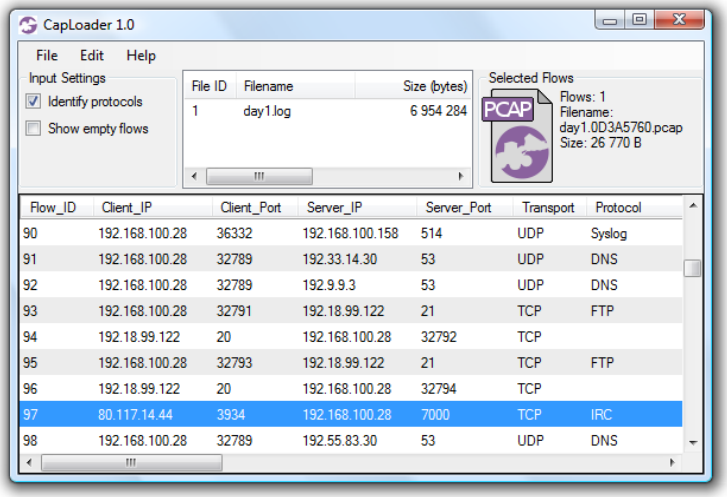


Illustration 4: CapLoader with "Protocol" column

The protocol identification feature is based on the SPID algorithm, which was developed by Erik Hjelmvik with initial funding from the Swedish Internet Infrastructure Foundation (.SE).

The CapLoader USB flash drive

CapLoader is delivered on a customized USB flash drive. CapLoader is a portable application, which means that it doesn't require any installation and can be run directly from the USB flash drive. Our recommendation is, however, that you copy the CapLoader directory to your local hard drive and run it from there for improved performance. It is up to you to decide if you will copy CapLoader to your computer's desktop, put it in your Program Files directory or place it in the root of your favorite HDD partition.

Illustration 5: CapLoader USB flash drive

4 Also known as “Port Independent Protocol Identification” (PIPI) or “Traffic Classification”

5 For example UDP 53 (DNS), TCP 80 (HTTP) or TCP 443 (SSL)