With Colasoft Capsa you can get an easy-to-use but advanced network traffic monitoring, protocol analysis and diagnosis software. It is a specialist to help us solve LAN troubles.

ARP broadcast, because of its simpleness, fastness, and effectiveness, is becoming increasingly popular among internet raggers, thus causing severe influence to the internet environment. With Colasoft Capsa, we can quickly and accurately locate the source of the attack when there is any ARP attack happens to our network, so as to ensure normal and reliable network operation.

We have four basic solutions to locate ARP attack with Colasoft Capsa:

- View ARP diagnosis events in the **Diagnosis** tab;
- View ARP request and response packets in the **Protocol** tab;
- View original information of ARP packets in the **Packet** tab;
- View node information in the **Physical Endpoint** tab;

Solution 1:

The **Diagnosis** tab is the most direct and effective place to locate ARP attack, and should be our first choice. Its interface is displayed as figure below.

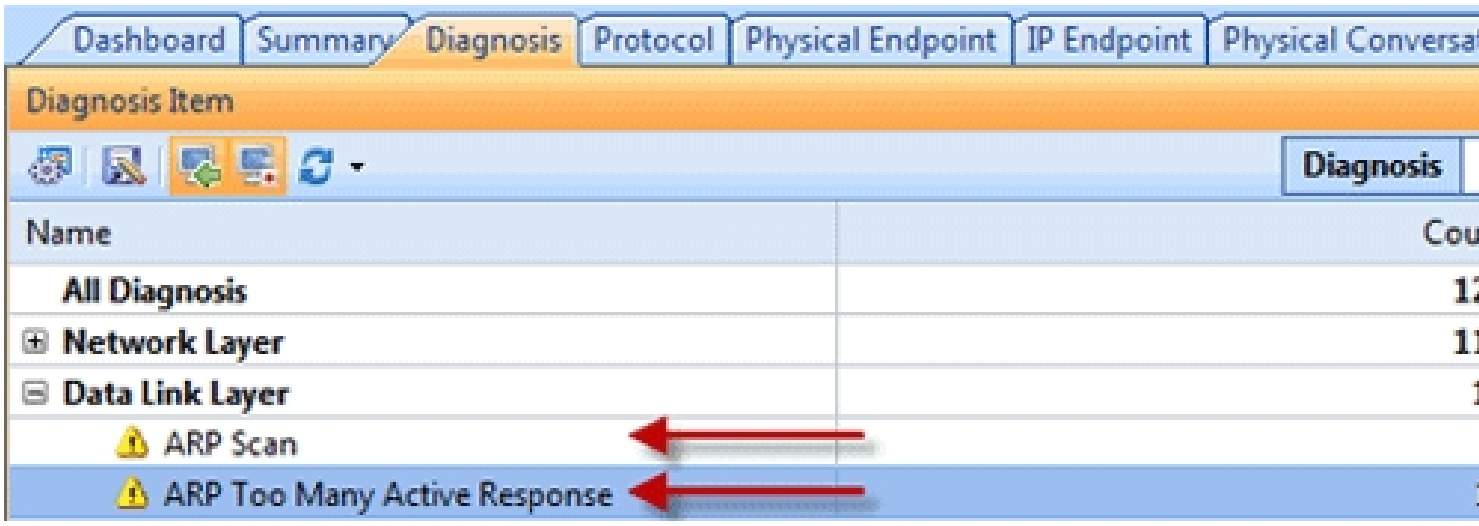


Figure 1: Diagnosis tab

Figure 1 definitely points out that there are two kinds of ARP attack event, **ARP Scan** and **ARP Too Many Active Response**, in the network, and the attack source is clearly given at the right panel. Meanwhile, Capsa will provide reasons of such ARP attacks and corresponding solutions.

Solution 2:

The status of ARP packets are displayed in the **Protocol** tab, like in Figure 2. Here we must pay special attention to the value of ARP **Request** and ARP **Response**. The ratio of ARP Request and ARP Request should be approximately 1:1 under general condition. If there is a great difference between these two values, there may be ARP attacks in the network.

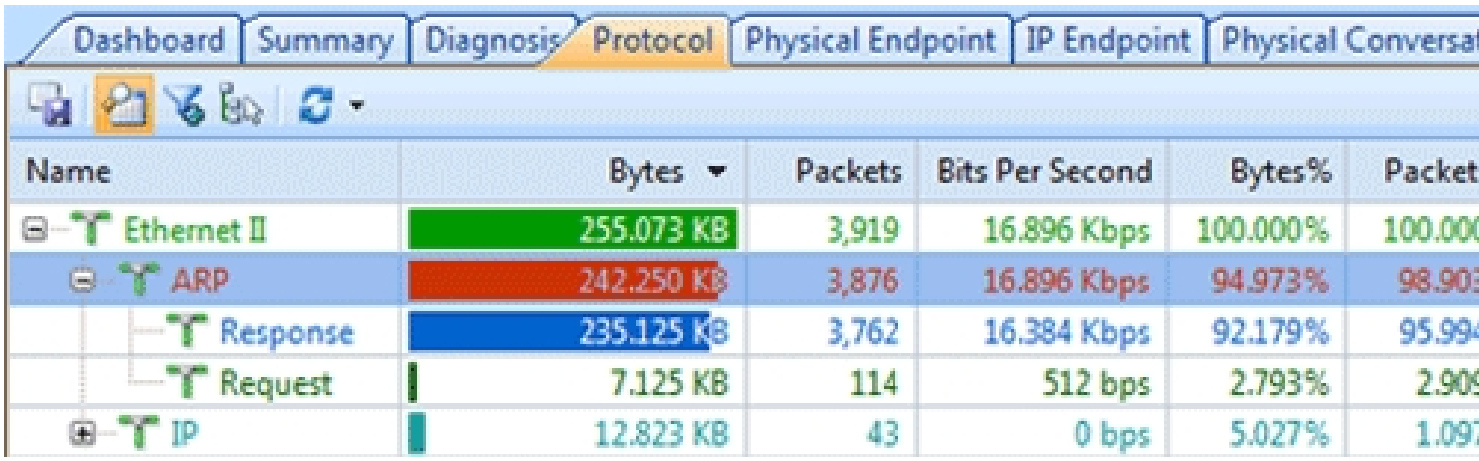


Figure 2: Protocol tab

In Figure 2 there are 3762 ARP Request packets but only 114 ARP Response packets, by

comparing these two values, we can presume there are ARP attacks in the network.

Solution 3:

Packet decoding information in the **Packet** tab can tell us the original information of ARP packets, please look at Figure 3.

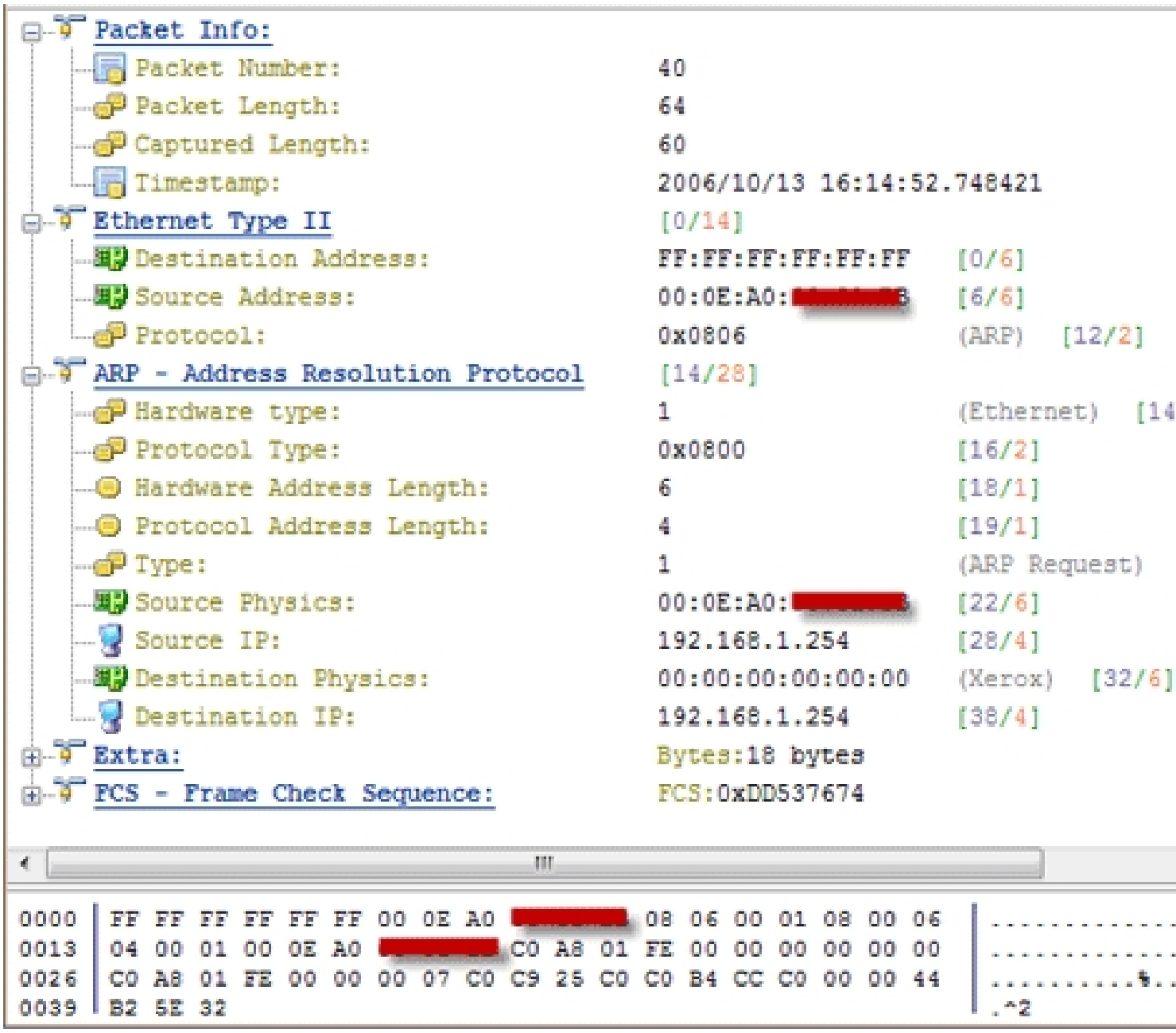


Figure 3: Packet tab

By decoding ARP packets, we can find out the source and destination of the ARP packets, the function and the reality of these ARP packets.

Solution 4:

Identify ARP attack in the **Physical Endpoint** tab (See Figure 4).

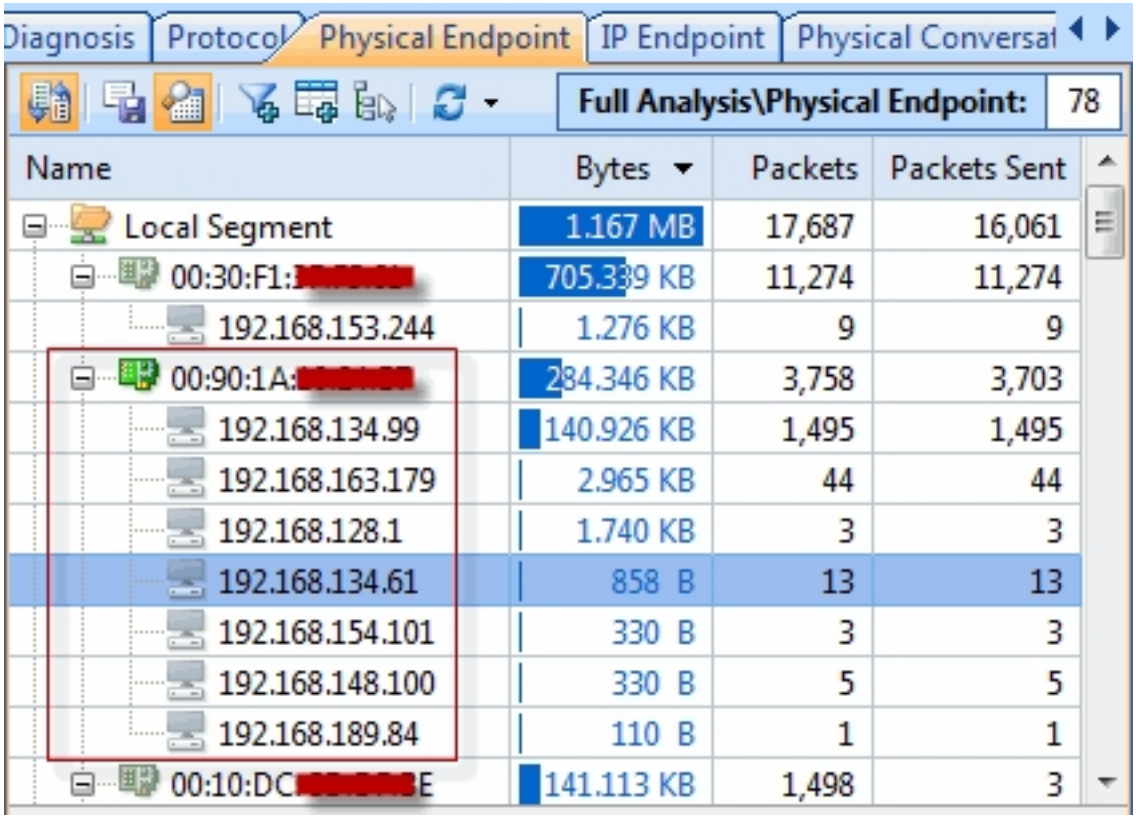


Figure 4: Physical Endpoint tab

In the **Physical Endpoints** tab we can view the correlation of MAC address and IP address. Generally speaking, one MAC address shall have only one IP address corresponding to it. If one MAC address has multiple IP addresses to it, the condition may be:

1. the host with the MAC address is the gateway;
2. these IP addresses are bound to the MAC address manually;
3. ARP attack

So, the **Physical Endpoint** tab can also give us a hint to locate ARP attack.

In addition, the **Matrix** tab allows us to see communication information between those hosts in the network, which helps us to fast identify abnormal conditions and locate the attack source.

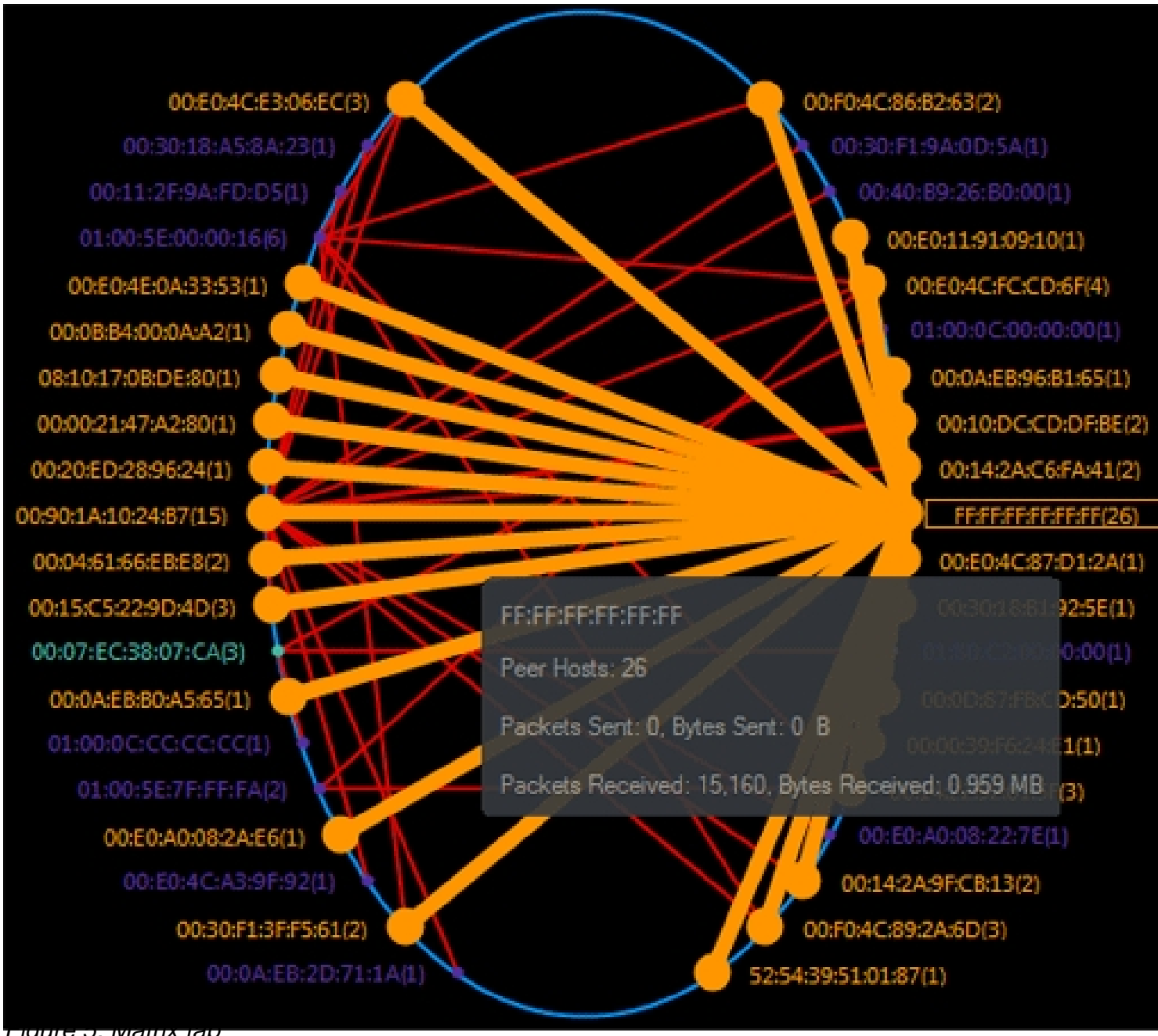


Figure 5: Matrix tab

Conclusion

ARP, as one of the most popular attacks in recent days, may cause severe problems to our network. How to fast troubleshoot ARP attacks is what every network administer concerns. Colasoft Capsa will greatly enhance network administrators' capability to identify ARP attacks and protect the network from ARP attacks, so as to ensure normal network operation. Besides fast locating ARP attacks, Colasoft Capsa can also analyze network abnormities, locate failure nodes, enhance network security, evaluate and improve network performance.