



## Digital Evidence

Axxera, a premier managed security services provider, offers Digital Evidence. In today's growing expansion of cyber crimes and cyber related theft, it is difficult for security professionals to assess in real time the exposure that their company could have due to a security breach.

Essentially, the Axxera Digital Evidence agent is a program that can see all of the information passing over the network it is connected to. As data streams back and forth on the network, the program looks and copies each packet from the source attacker and destination victim.

### What is Digital Evidence?

Normally, a computer only looks at packets addresses and ignores the rest of the traffic on the network. The digital evidence agent network interface is set to promiscuous mode. This means that it is looking at everything that comes through. The amount of traffic largely depends on the location of the computer in the network. A client system out on an isolated branch of the network sees only a small segment of the network traffic, while the main domain server sees almost all of it.

The Digital Evidence agent is usually set up in a filtered mode:

- Filtered - Captures only those packets containing specific data elements from the attacker and victim systems.

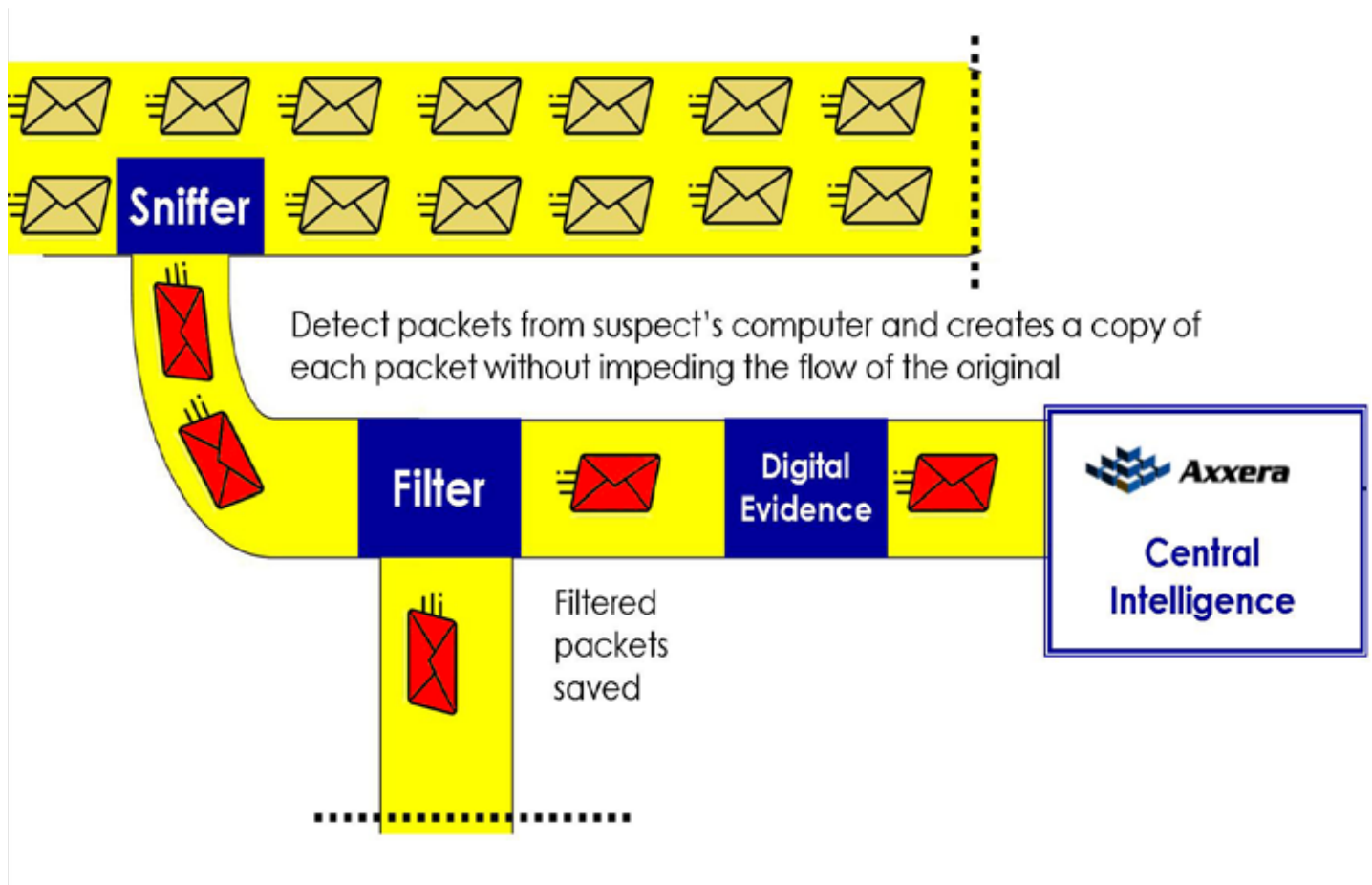
Packets that contain targeted data are copied as they pass through the system. The program stores the copies in a PCAP file. So that they can be analyzed carefully for specific information or patterns. A digital evidence agent located on your network would be able to monitor suspicious traffic activities such as:

- Which Web sites the attacker visited
- What the attacker looked at on the site
- Whom the attacker sent e-mails to
- What is in the e-mail the attacker sent
- What the attacker download from a victim system
- What streaming events the attacker used, such as audio, video and Internet telephone

#### Features of Digital Evidence:

- Suspicious traffic gathering agent
- Real-time gathering of attacker and victim raw packets
- Packets saved to PCAP file for further analysis
- Reconstruction and analysis of communication
- Reconstruction of email sent
- Reconstruction of web page viewed
- Reconstruction of audio and video files
- Reconstruction of transfered files
- Risk Analysis
- Evidence for law enforcement investigation

Figure A: Digital Evidence architectural flow



### How does it work?

Now that you know a bit about what the Digital Evidence is, let's take a look at how it works:

1. The Central intelligence system has reasonable suspicion that someone is engaged in suspicious traffic activities.
2. The Central Intelligence system configures the agent with the IP Address of the suspect so that the agent will only capture packets from this particular location. It ignores all other packets.
3. Digital Evidence copies all of the packets from the suspect's system without impeding the flow of the network traffic.
4. Once the copies are made, these packets are saved to a PCAP file and sent into the Central Intelligence Portal.
5. Once the Central Intelligence receives the evidence it is added to the security incident for authorized analysis of the data.
6. Once the data is analyzed and reviewed the security incident can be escalated to the local law enforcement district office.
7. If the results provide enough evidence, law enforcement can use them as part of a case against the suspect.

## Additional Security Offerings

Central Intelligence offers a full suite of information security services to suit your needs. For additional information about Central Intelligence's Real-Time Managed Security Services, see the following documents:

- Managed and Monitored Firewall Service
- Managed and Monitored Network Based IDS Service
- Host-Based IDS Monitoring Service
- Predictive/Proactive Security Service
- Enterprise Security Reporting

## Protect Your Network with Central Intelligence's Managed and Monitored Security Services

With real-time information protection and industry-leading security professional services, Central Intelligence provides the most advanced information security available today. Find out how Central Intelligence's Managed and Monitored Security Services can give your network the Proactive security you need.

### About Axxera

Founded in 2007, Axxera is uniquely positioned to safeguard the electronic presence of today's corporations. Our founders pioneered the security industry by designing, and building security infrastructure worldwide. Axxera has helped secure hundreds of global organizations, and e-businesses.

Axxera Managed Security Services delivers the expertise, tools and infrastructure you need to secure your information assets from Internet attacks 24/7/365, often at a fraction of the cost of in-house security resources. Access to the Axxera Portal a secure Web-based management tool, provides a single interface to easily monitor the security of your overall infrastructure of managed and unmanaged security devices.

Axxera's proprietary technology platform enables detailed processing of every event on your network. Our processing model gives expert analysts at Axxera's Security Operations Centers the advanced tools they need to provide real-time analysis and protection.

#### Axxera Headquarters

---

2 Park Plaza	Phone: 949.502.4930
Suite 200	Fax: 949.861.9229
Irvine, CA. 92614	Email: info@axxera.com
	Web: www.axxera.com

#### Sales Offices

---

3109 Colebrook Lane	590 Madison Avenue
Dublin, CA. 94568	New York City, NY. 10022

#### Axxera International Center

---

1st Floor, Lakshmi Towers - B  
Plot No. 17, Nagarjuna Hills  
Hyderabad, Andhra Pradesh, India.  
Pin - 500082