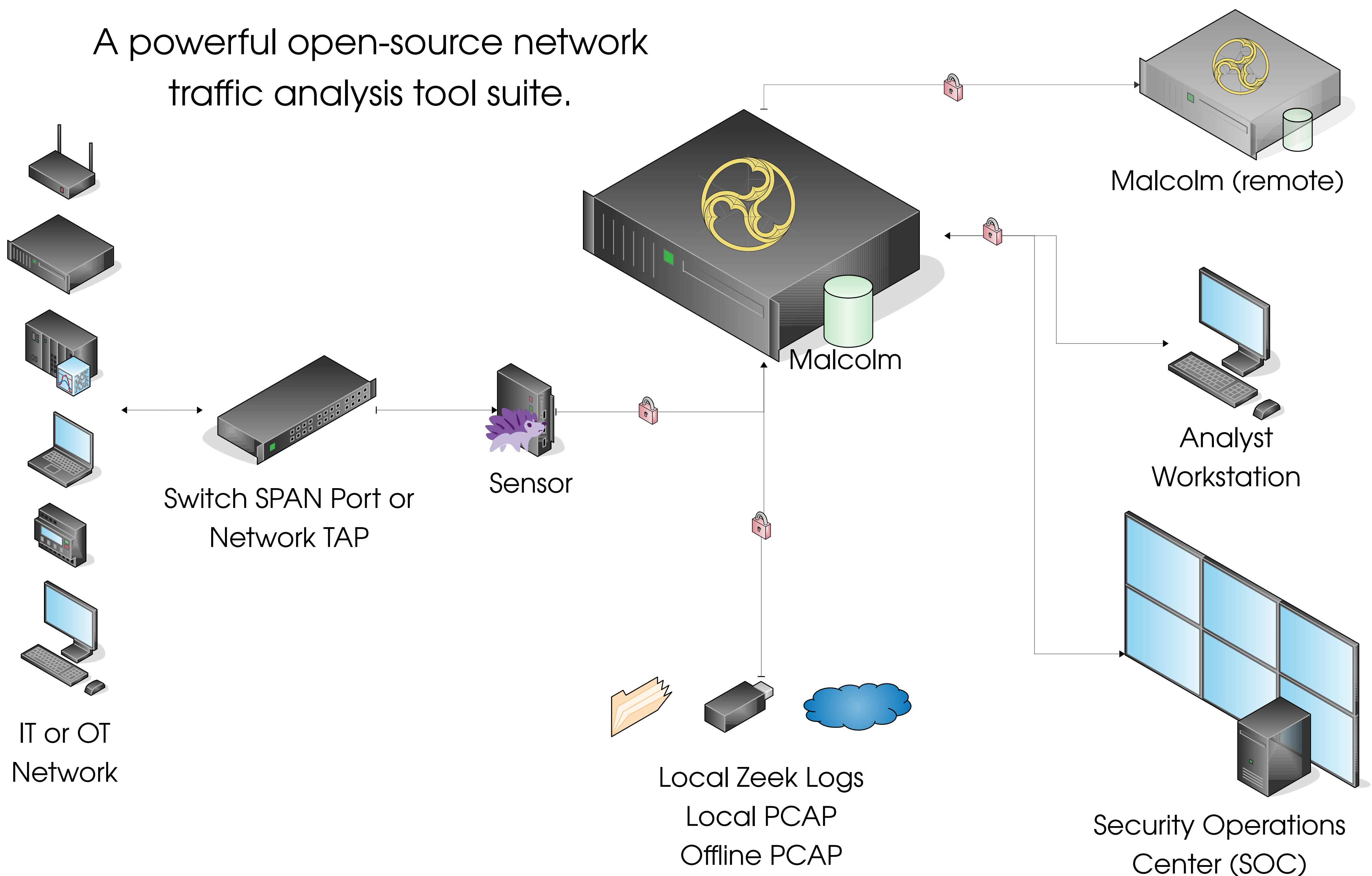


# Malcolm

<https://github.com/idaholab/Malcolm>

A powerful open-source network  
traffic analysis tool suite.



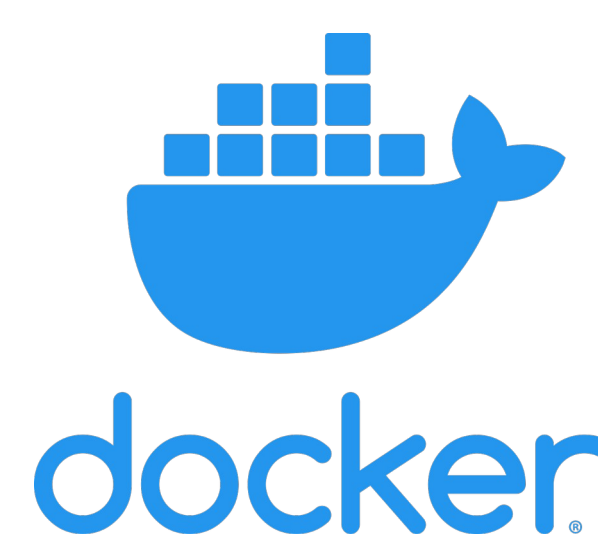
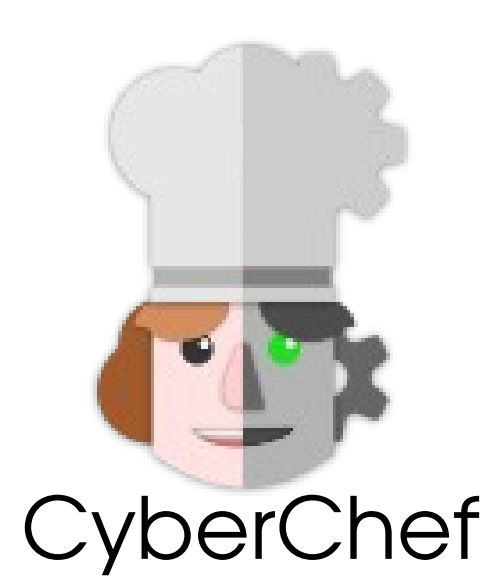
## Supported Protocols

Internet layer  
Border Gateway Protocol (BGP)  
Building Automation and Control (BACnet)  
Bristol Standard Asynchronous Protocol (BSAP)  
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC)  
Dynamic Host Configuration Protocol (DHCP)  
Distributed Network Protocol 3 (DNP3)  
Domain Name System (DNS)  
EtherCAT  
EtherNet/IP / Common Industrial Protocol (CIP)  
FTP (File Transfer Protocol)  
Google Quick UDP Internet Connections (gQUIC)  
Hypertext Transfer Protocol (HTTP)  
IPsec  
Internet Relay Chat (IRC)  
Lightweight Directory Access Protocol (LDAP)

Kerberos  
Modbus  
MQ Telemetry Transport (MQTT)  
MySQL  
NT Lan Manager (NTLM)  
Network Time Protocol (NTP)  
Oracle  
OpenVPN  
PostgreSQL  
Process Field Net (PROFINET)  
Remote Authentication Dial-In User Service (RADIUS)  
Remote Desktop Protocol (RDP)  
Remote Framebuffer (RFB / VNC)  
S7comm / Connection Oriented Transport Protocol (COTP)  
Session Initiation Protocol (SIP)

Server Message Block (SMB) / Common Internet File System (CIFS)  
Simple Mail Transfer Protocol  
Simple Network Management Protocol  
SOCKS  
Secure Shell (SSH)  
Secure Sockets Layer (SSL) / Transport Layer Security (TLS)  
Syslog  
Tabular Data Stream  
Telnet / remote shell (rsh) / remote login (rlogin)  
TFTP (Trivial File Transfer Protocol)  
WireGuard  
tunnel protocols (e.g., GTP, GRE, Teredo, AYIYA, IP-in-IP, etc.)

Malcolm provides an easily deployable network analysis tool suite for full packet capture artifacts (PCAP files) and Zeek logs by leveraging several industry-standard open source tools, including:



... and  
more!