MCR CAPTOR

Given the increasing use of Internet, LEAs need a Monitoring Center capable to effectively carry out IP interceptions, which nowadays represent a strategic tool to provide a real added value to investigation activities.
AREA has developed the MCR CAPTOR family of probes to support LEAs in their LI (Lawful Interception) activities requiring IP data acquisition; MCR Captor probes are totally integrated in the MCR Voice & Data Monitoring Center.

MCR Captor IP Probes installed in an ISP network allow to:

- acquire IP streams up to 10 Gbps
- apply real time filtering rules to extract specified IP sessions
- forward captured content to MCR Server

MCR CAPTOR INTEGRATION

MCR Captor family of probes is fully integrated with other MCR Voice and Data Monitoring Center components, providing complete Communication monitoring and analysis functionalities.

Probes Management

Centralized installation provides GUI interface to manage the whole system of MCR Captor probes deployed in the network, configure Targets, and monitor health status.

Content Inspection and Analysis

MCR Player provides extensive functionalities to access CC and CDR of intercepted targets, being them IP or Voice, offering advanced features for decoding, presenting and filtering of data. MCR Studio is the data-mining tools to analyze target's social relationships and build personalized analysis patterns.

Centralized Storage

MCR Server provides storage, security and anti-tampering signature on recorded data, accordingly to specific country legislation requirements

MCR CAPTOR TARGET DEFINITION

MCR Captor enables LEAs to use different approaches to IP data interception.

Investigation Approach

This approach is usually based on the monitoring of well known targets, previously identified by means of investigation, in order to collect evidences, discover social relationships and find hints to create other targets.
The triggering rule can be an IP address, a Radius Login ID, an e-mail address, a chat or a VoIP ID or telephone number, etc.

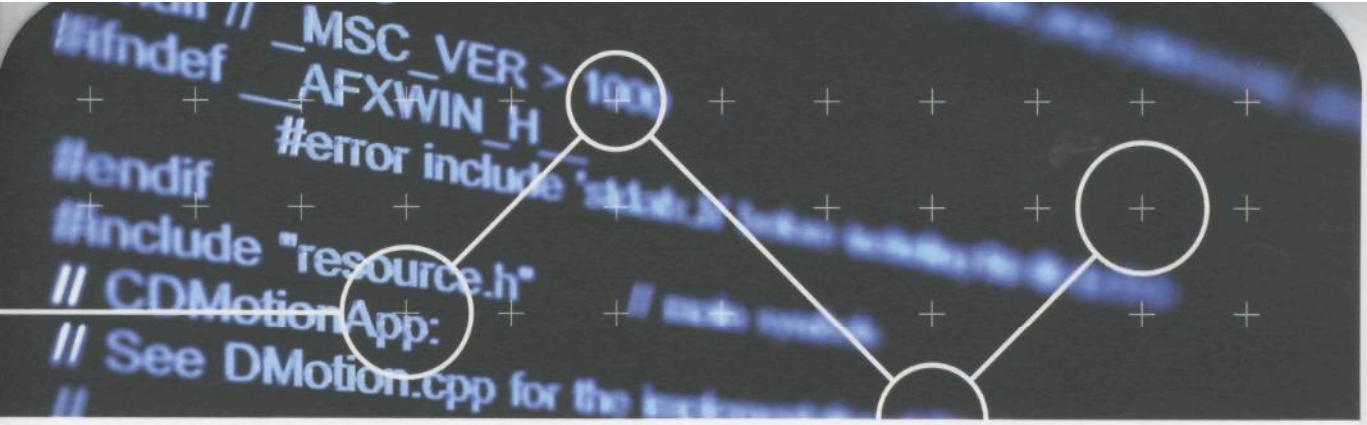
Intelligence Approach

This approach is usually based on the monitoring of communication content of targets that are not identified yet. This kind of interception applies in Crime Prevention and Homeland Security, as it is useful both to discover suspect behaviors and to identify the subjects they belong to, by means of content monitoring.
The target can be email subject, chat content, generic word spotting in complete stream, type of communication protocol, etc..

Trigger Table

This table presents a summary describing the most common target definition of MCR Captor

TYPE OF TARGET	TARGET DEFINED BY
Target oriented	IP address / Radius ID / E-mail address / Chat ID / VoIP ID / Telephone number / URL / DNS Queries /... /
Content Oriented	Email (Subject and body) / Webmail (Subject and body) / Instant Messaging / Social Network Chat / Web Pages / Generic Word Spotting in full stream / ..../
Communication Type Oriented (Identification of protocols)	Mail / Webmail / HTTP / VoIP / Chat / Communication Port / Encrypted Protocols (Skype, HTTPS...) / Peer 2 Peer / ... /



MCR CAPTOR APPLICATION SCENARIOS

Example 1: Pirate Web Site

An example is the monitoring of a pirate web site traffic. LEAs requirement was to trace every access to a pirate website, and collect all the traffic generated by those users, to discriminate relevant targets from occasional visitors.
The constraint in this process is the capability to automatically target the web site which was not always on-line and whose IP address was dynamic.
Establishing a trigger monitoring DNS traffic allowed to identify those IP addresses accessing the specific web site; those IP Addresses were addressed as targets, from that point on, capturing entire traffic generated, allowing LEAs to identify relevant users, and obtain their ID (email, chat...)

Example 2: Word Spotting (protocol based)

MCR Captor can process a whole aggregated IP stream and extract the contents (such as HTTP pages or e-mails) in which specified words are detected. Moreover, in order to focus on specific communications channel, the combination of more triggers is extremely important. In this experience LEAs, needed to search specific words, but to limit false positive matches, traffic analyzed was restricted to Instant Messaging, Webmail and Mail protocols.

INTEROPERABILITY, STANDARD AND INTEGRATION INTO TARGET NETWORKS

MCR Captor enables LEAs to monitor IP contents through any kind of fixed and mobile data networks: dial-up, xDSL or fiber (fixed networks), and WLAN, GPRS, EDGE or UMTS (mobile networks). MCR Captor probes are configured to fit the network technology adopted by Telco operators (i.e. GB Ethernet, STM, PoS) and can capture high bit rate IP streams (up to 10 Gbps) through SPAN ports or by means of tapping devices.
AREA monitoring system is compliant to emerging LI standards such as ETSI (TS 101 671, TS 102 232) and CALEA, yet MCR Captor is widely adaptable to fit Vendor-specific or Country-specific interception scenarios.

FLEXIBILITY AND SCALABILITY

MCR Captor can be easily adapted to all the changes that can occur in number of monitored targets, protocols and ISP network modifications.
MCR Captor can support interception activities carried out simultaneously by different LEAs thanks to the capability to manage a huge number of concurrent interception instances.

MCR CAPTOR MAIN FEATURES

System reliability

MCR adopts an advanced automatic backup policy and a RAID 5 mechanism is configured on probes to avoid data loss. Moreover the handover capability is redounded in order to avoid that a single fault can affect the whole system recording capacity.

Security

MCR Captor is configured to be protected from any virus threats, malware in general and hackers attacks.
On probes, servers and workstations a top-level anti-virus software is installed and a firewall infrastructure is properly configured according to the latest policies issued by authoritative IT security companies and communities.