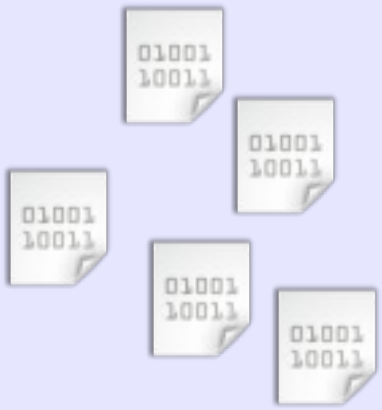
Xplico

Internet Traffic Decoder
Network Forensic Analysis Tool

Scopo del progetto

Riuscire a estrarre (e a visualizzare) i dati applicativi trasportati dalla rete.

- pagine web
- email
- chat
- …



pcap

Problematiche

Si devono affrontare due distinti insiemi di problemi

- l'acquisizione dei dati
- la decodifica-ricostruzione dei dati

Acquisizione:

Cattura di tutti i dati/pacchetti che trasportano l'informazione da estrarre ed eventuali correlazioni fra i dati/pacchetti.

Problemi:

- elevata velocità delle reti e conseguente mole di dati
- archiviazione dei dati in real-time

I problemi sono analoghi a quelli che si riscontrano in altri ambiti. I progetti nProbe e nTop propongo un approccio che spazia dall'utilizzo di appositi moduli kernel all'integrazione con HW dedicato.

Decodifica-Ricostruzione

Requisiti:

- tutti i dati che compongono l'informazione da estrarre
- avere le specifiche dei protocolli: RFC, ETSI, reverse engineering, …
- possedere le informazioni "aggiuntive" per l'estrazione dei dati

Non è essenziale imporre il vincolo di real-time all'elaborazione

Trasporto dell'Informazione

L'informazione da estrarre la si può trovare trasportata in rete in varie forme e modalità

- HTTP, POP, IRC, … : con un unico flusso TCP
- VoIP (SIP, H323, MEGACO, ...): più “flussi” ma limitati in numero
- FB Web chat, Paltalk Express, ..: trasportati dal HTTP in più messaggi e su più flussi, in un arco temporale che possiamo però considerare limitato
- P2P: molti “flussi” distribuiti anche in un ampio arco temporale

In alcuni casi la sola estrazione del dato non è sufficiente, un esempio sono le pagine Web

Sistema di decodifica-ricostruzione

L'obiettivo che volevamo raggiungere:

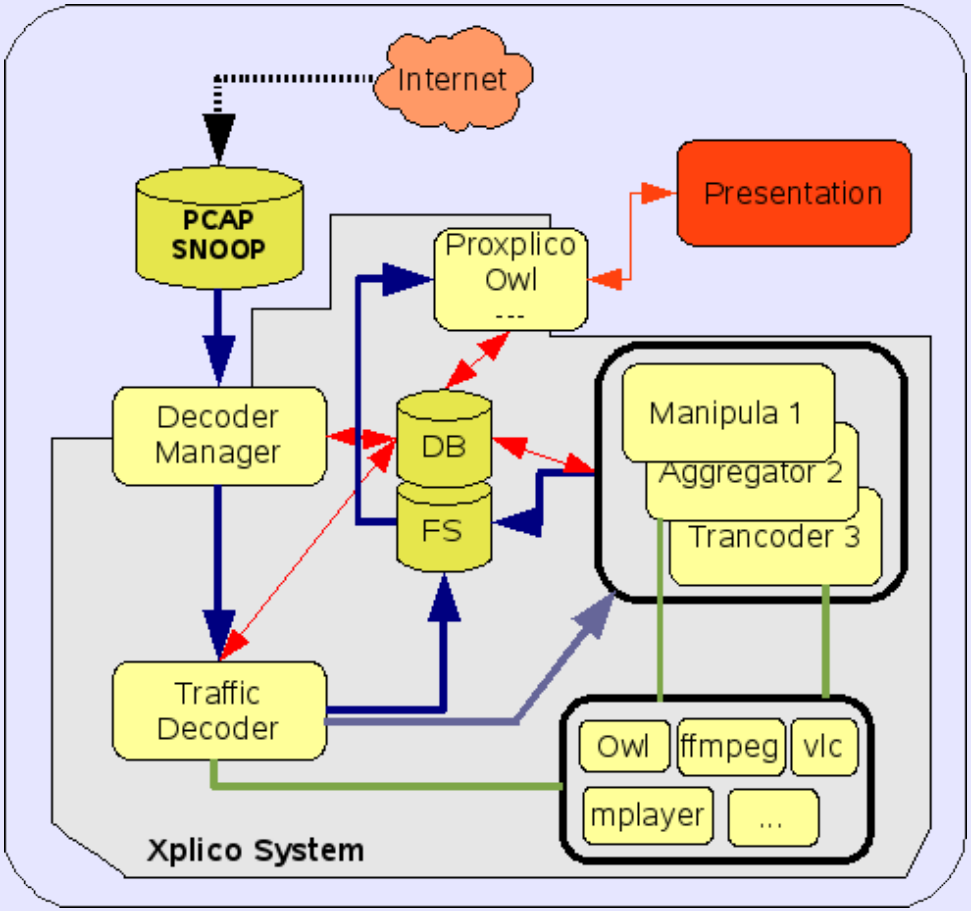
- rendere disponibile un sistema e non unicamente un “decodificatore”
- fornite anche un'applicazione di decodifica stand alone
- facilitare l'integrabilità

Progetti con analoghe funzioni:

- PyFlag
- Packet-o-Matic

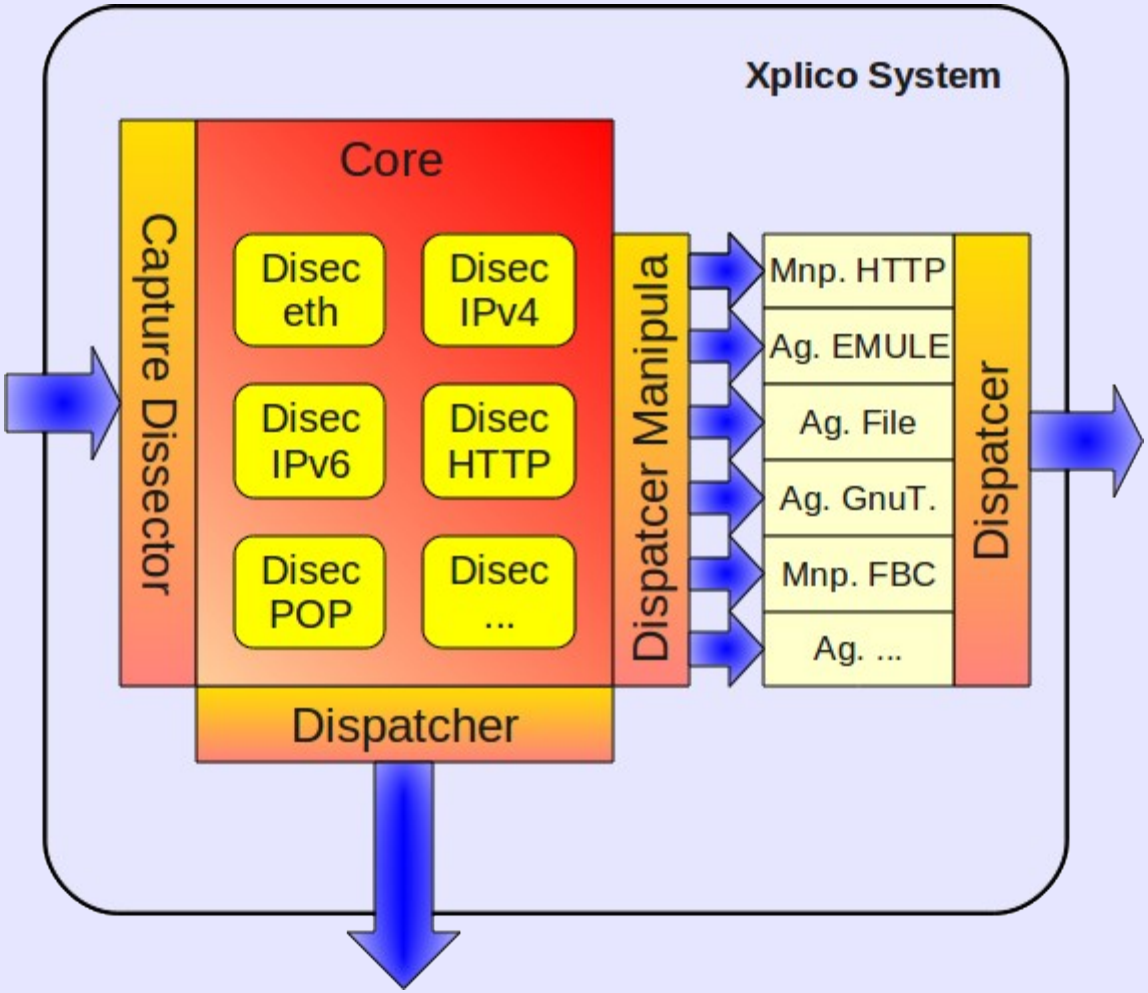
Xplico System

Sistema “chiavi in mano”, con la collaborazione di Stefano Fratepietro di Deft Linux



- Dema
- Xplico
- Manipolatori (/Aggregatori)
- XI

Xplico & Manipulator

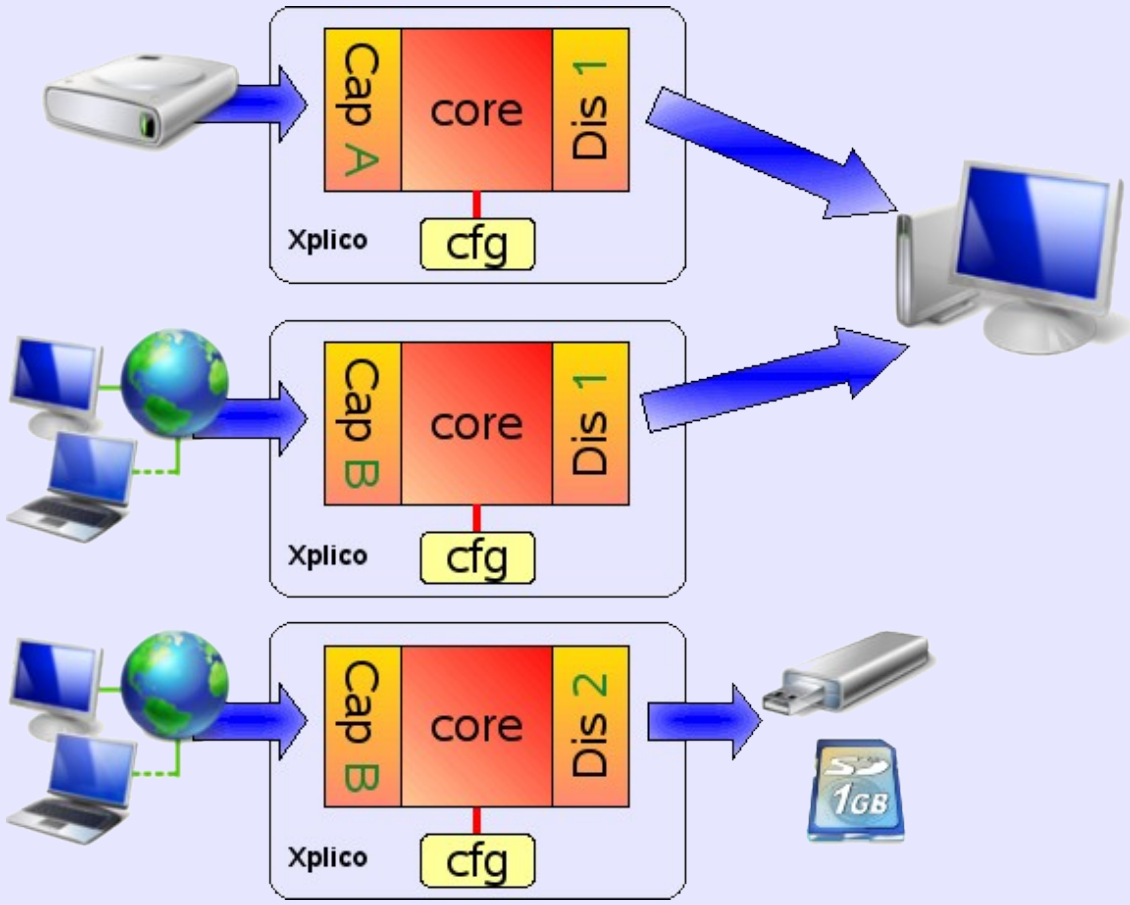


Modularità:
- input
- output
- dissector

Indipendenza sia dalla forma dei dati in ingresso che della forma dei dati desiderata in uscita

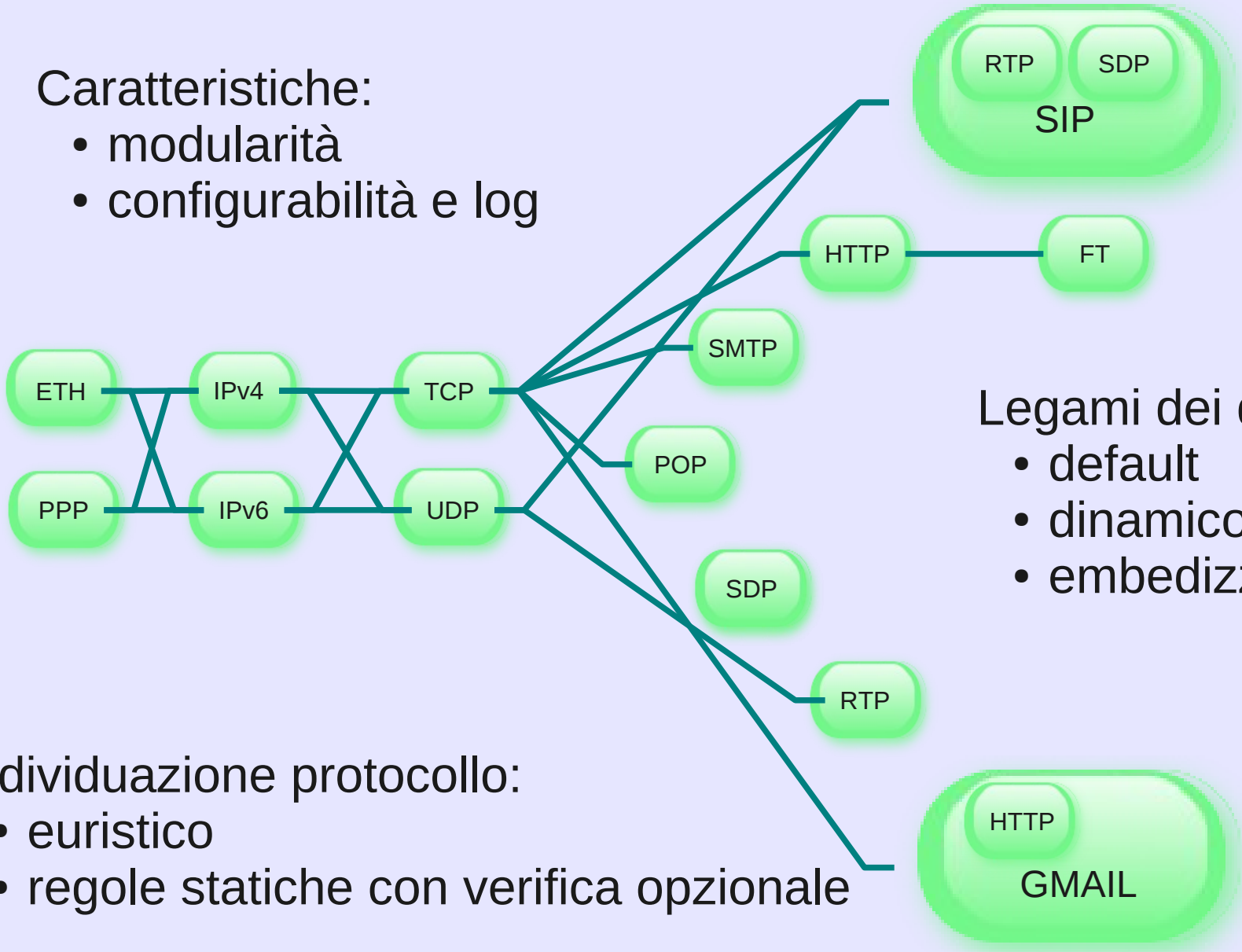
Tutto ruota attorno alle possibili forme del “flusso d'informazione”

Flessibilità nell'Input e nell'output



Dissector

Caratteristiche:
- modularità
- configurabilità e log



Legami dei dissector:
- default
- dinamico
- embedizzato

Individuazione protocollo:
- euristico
- regole statiche con verifica opzionale

Protocolli

HTTP
- ricostruzione pagina web con emulazione della cache
- riassemblaggio di file scaricati in modo frammentato

POP, IMAP, SMTP, SIP, RTP, RTCP, DNS, FTP, TFTP, NNTP, Telnet, MMS

FB Web chat, IRC, MSN, Paltalk, Paltalk Exptess

In futuro: P2P e altre Chat

Riferimenti

Siti:
http://www.xplico.org
Forum: http://forum.xplico.org
Wiki: http://wiki.xplico.org

Distribuzioni:
DEFT Linux: http://www.deftlinux.net
BackTrack: http://www.backtrack-linux.org

Gianluca Costa
Email: g.costa@iserm.com