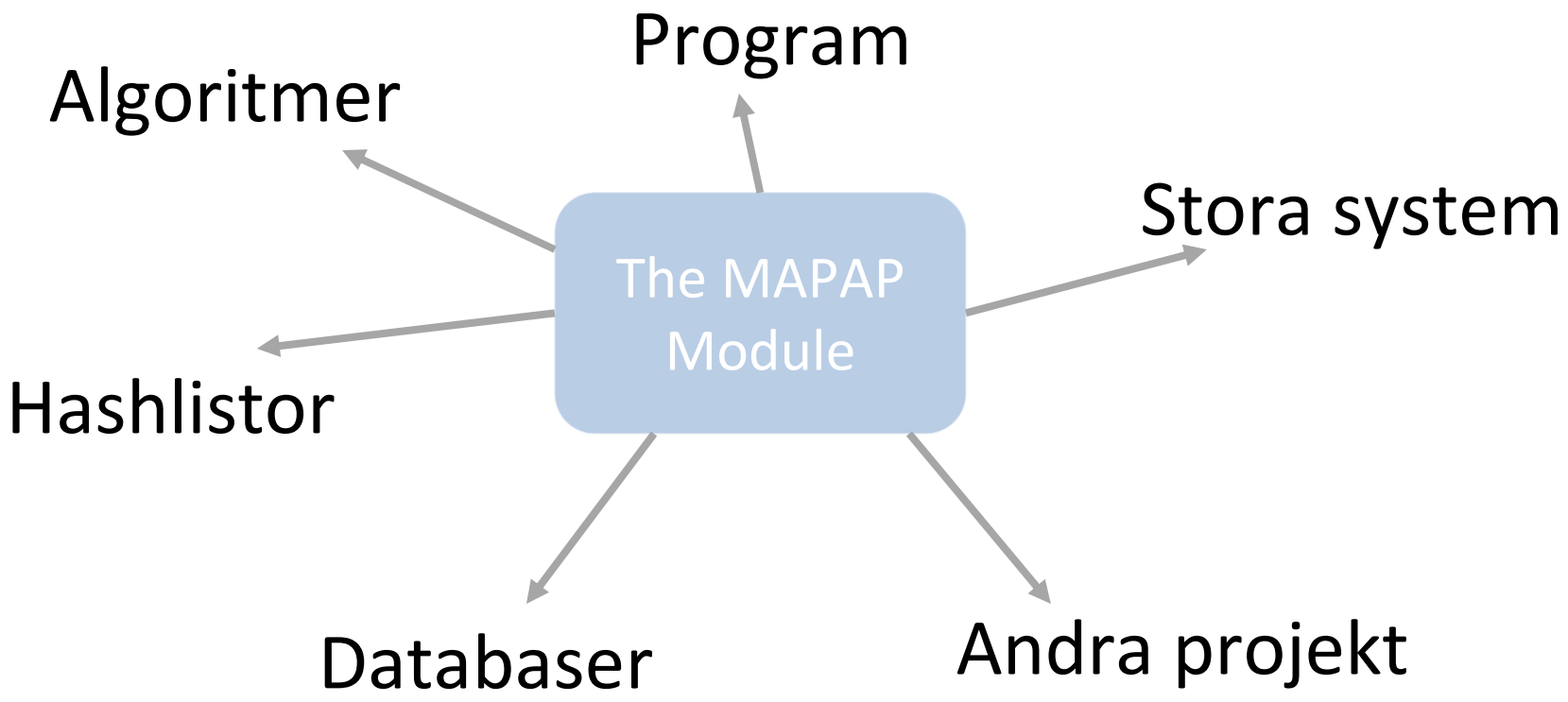
The MAPAP Module

Ett examensarbete av
Daniel Melani
och
Therese Axelsson

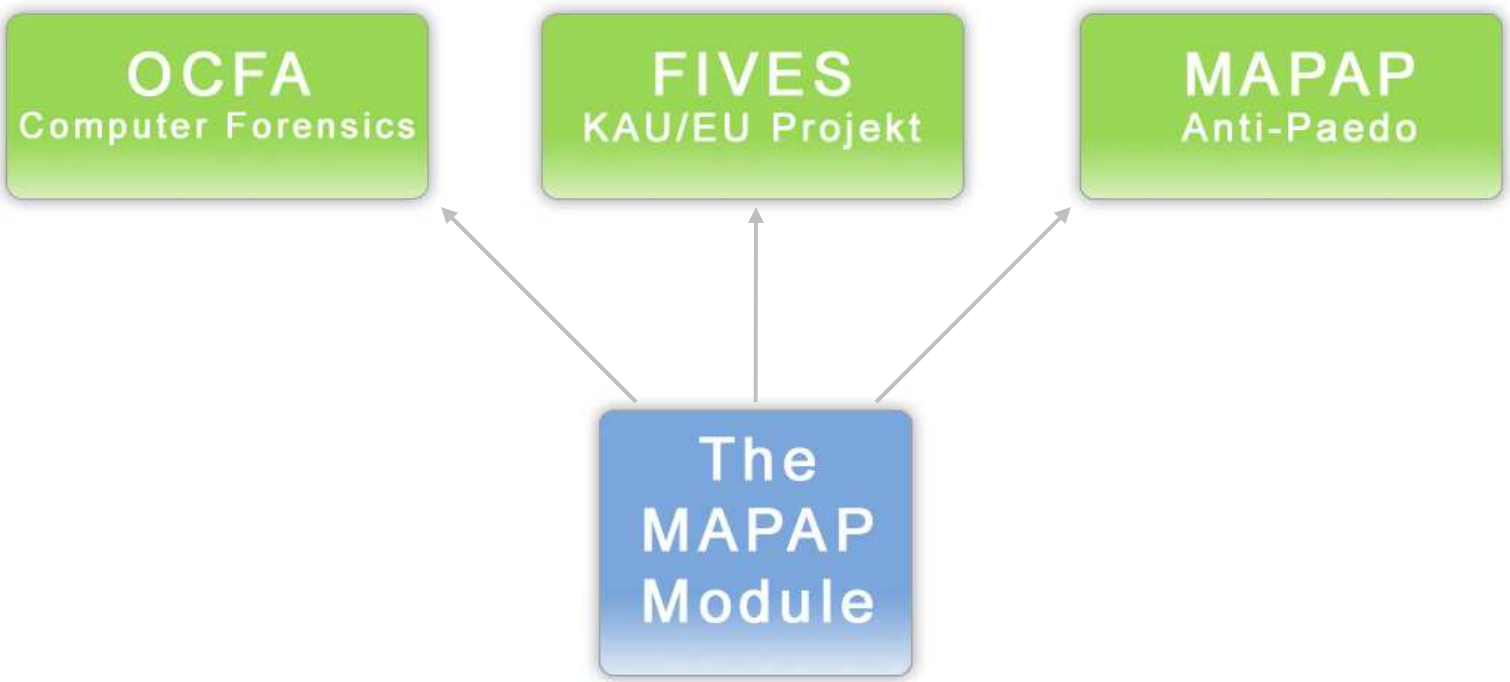
Agenda

- Översikt – Projektet
- Före – Hur allt började
- Under – Utveckling och implementation
- Efter – Resultatet
- Nu – Frågor och diskussion

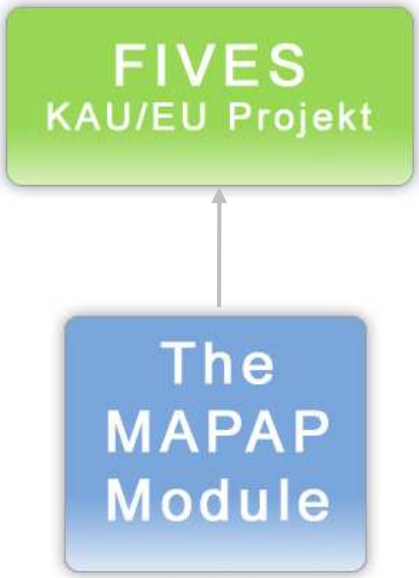
Vad är The MAPAP Module?



Relationer

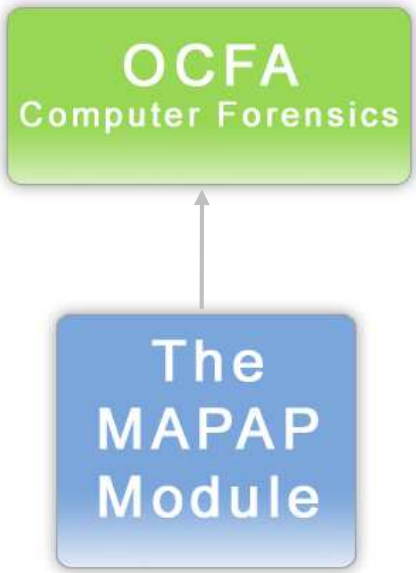

OCFA
Computer Forensics
FIVES
KAU/EU Projekt
MAPAP
Anti-Paedo
The
MAPAP
Module

FIVES



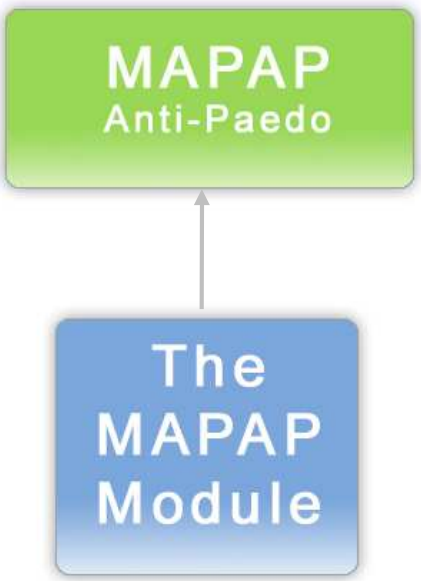
- Forensic Image and Video Examination Support
- EU-finansierat
- Karlstad Universitet är koordinator
- Nya verktyg för att bekämpa barnpornografi
- Fokus på mediafiler
- Beställare av The MAPAP Module

OCFA



- Open Computer Forensic Architecture
- Ramverk för att hantera datarelaterat bevismaterial
- Open Source
- Linux / POSIX-standard
- Moduler/Program
- Omfattande bibliotek
- Routing
- Databaser PostgreSQL/Berkeley DB

MAPAP



- Measurement and Analysis of P2P activity Against Paedophile content
- Lokalisera barnpornografi
- Vilseledande nyckelord
- Filtrera peer to peer-nätverk
- Gradera sannolikhet för barnpornografi
- Tillgodoser insamlad data

The MAPAP Module - Intro

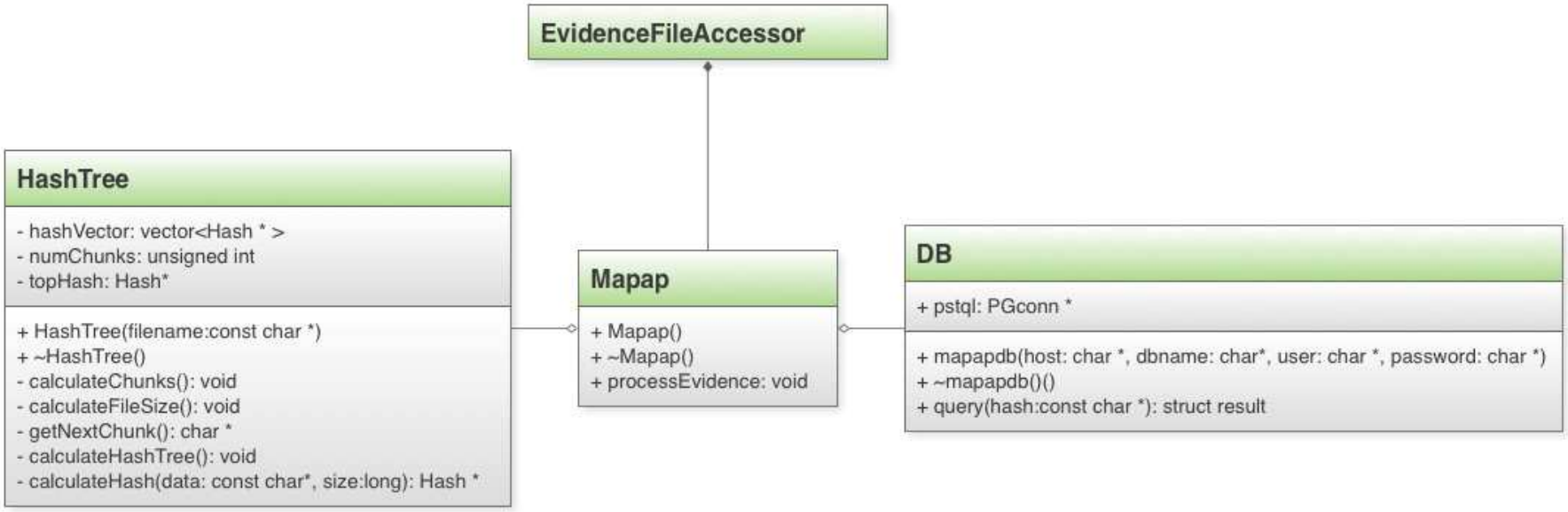
Kortfattat utför The MAPAP Module dessa uppgifter:

- Hämtar bevis från OCFA
- Skapar hashfil
- Jämför med hashfiler från MAPAP
- Sparar resultat/gradering
- Skickar tillbaka till OCFA

The MAPAP Module - Teknik

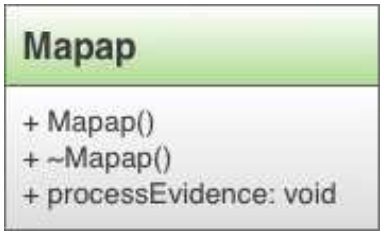
- C++ / PERL
- Eclipse
- Debian
- PostgreSQL

The MAPAP Module - Design



UML-diagram av modulen

The MAPAP Module - Mapap

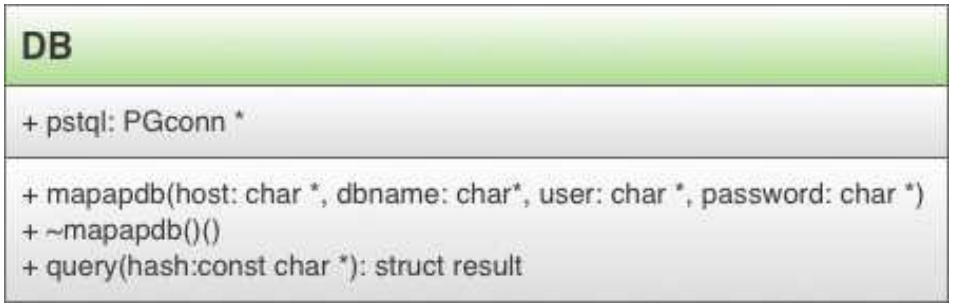


- Kopplar samman med OCFA
- Tar emot bevisdata
- Sköter flödet i programmet/modulen
- Skickar tillbaka resultat

The MAPAP Module - HashTree

- Delar upp filen i block
- Räknar ut en hash för varje block separat
- Sätter samman en topp-hash
- Sparar undan topp-hashen

The MAPAP Module - DB



- Skapar koppling mot databas
- Tar emot SQL-fråga
- Ställer frågan mot databasen
- Skickar tillbaka resultatet

The MAPAP Module - Resultat

Testning

- Goda testresultat
- Inget minnesläckage
- Fungerande felhantering

Framtiden

- Bäddad för framtida utveckling
- Enkelt implementerad
- Följer OCFA-standard

Frågor

Diskussion