European Antitrust Forensic IT Tools

Nino Vincenzo Verde

Dipartimento di Informatica
Universita` di Roma "La Sapienza"
113 Via Salaria, 00198 Roma, ITALY
email: verde@di.uniroma1.it

About me

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Dipartimento di Informatica della Facoltà di Ingegneria dell'Informazione, Informatica e Statistica dell'Università degli Studi di Roma "La Sapienza"

- Primo appuntamento sui temi del Master:
  - **Come:** Tavola rotonda "Cybercrime e Informatica forense: errori, professionalità e ambiti di applicazione"
  - **Dove**: Aula alfa, via Salaria 113
  - **Quando**: 28/4/2015 ore 16-19
  - **Discussant:** esponenti della Corte di Cassazione, Procura, Polizia Postale, Albo psicologi, etc.
- **Info**: mastersicurezza@di.uniroma1.it

Obiettivi del master

- Promuovere una professionalità multidisciplinare che integri le competenze, attualmente scisse nel mondo della formazione, del settore informatico, giuridico e psicologico

- Sviluppare un profilo di esperienza che possa intervenire, con una competenza analitica, tecnico-investigativa in ambito giudiziario, aziendale e nella pubblica amministrazione

Aree tematiche principali

- Computer Security and Computer Forensics
- Malware Analysis and Investigation
- Mobile Device Forensics
- Live Data Forensics
- Money Laundering Investigations
- Criminal profiling and crime investigations
- Risk analysis for reputation preservation
- Big Data e Data Mining
- Enterprise Reputation and Risk Management

Outline of the talk

- Introduction about the antitrust activities
- International context of the project
- The EAFIT_TOOLS project
  - Objectives
  - Project phases
  - Peculiarities of the Antitrust Investigations
- EAFIT_TOOLS indexing software
- Final remarks

Introduction about the Antitrust Activities

- **Competition** encourages companies to offer consumers goods and services at the most favourable terms
  - Anticompetitive practices cases
  - Abuse of dominance cases
- **Cartels**:
  - is a specific type of antitrust enforcement.
  - A cartel is a group of similar, independent companies which join together to fix prices, to limit production or to share markets or customers between them.

Introduction about the Antitrust Activities

- **Competition** encourages companies to offer consumers goods and services at the most favourable terms
  - Anticompetitive practices cases
  - Abuse of dominance cases
- **Cartels**:
  - is a specific type of antitrust enforcement.
  - A cartel is a group of similar, independent companies which join together to fix prices, to limit production or to share markets or customers between them.
- **Terminology:**
  - **Competition Authority (CA) = Antitrust**

Fighting against cartels: typical workflow

Fighting against cartels: typical workflow

LENIENCY
PROGRAM

Fighting against cartels: typical workflow

LENIENCY
PROGRAM

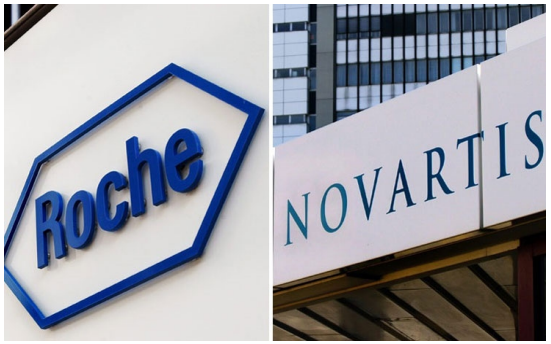
Fighting against cartels: typical workflow

LENIENCY PROGRAM

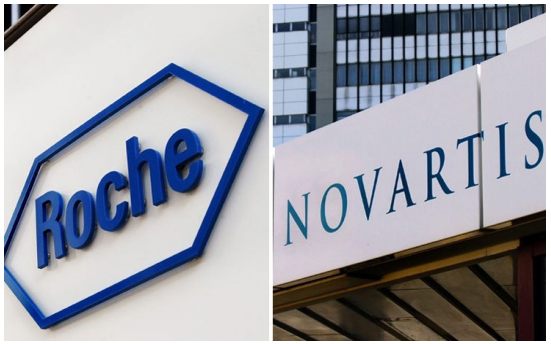
TRIAL

Examples of Fines: AGCM – Italy (2014)

Examples of Fines: AGCM – Italy (2014)



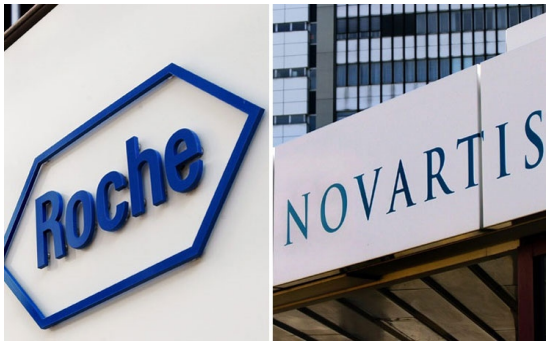
Examples of Fines: AGCM – Italy (2014)



I due gruppi si sono accordati illecitamente per ostacolare la diffusione dell'uso di un farmaco molto economico, Avastin, nella cura della più diffusa patologia della vista tra gli anziani e di altre gravi malattie oculistiche, a vantaggio di un prodotto molto più costoso, Lucentis, differenziando artificiosamente i due prodotti.

Per il Sistema Sanitario Nazionale l'intesa ha comportato un esborso aggiuntivo stimato in oltre **45 milioni** di euro nel solo 2012, con possibili maggiori costi futuri fino a oltre **600 milioni** di euro l'anno.

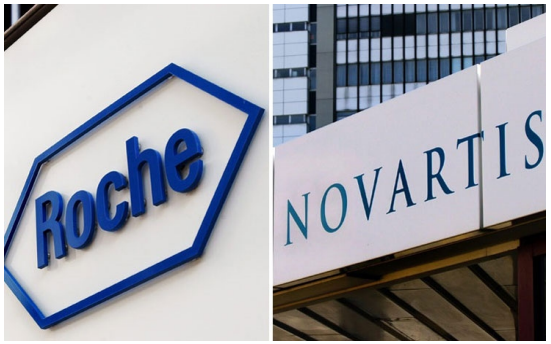
Examples of Fines: AGCM – Italy (2014)



I due gruppi si sono accordati illecitamente per ostacolare la diffusione dell'uso di un farmaco molto economico, Avastin, nella cura della più diffusa patologia della vista tra gli anziani e di altre gravi malattie oculistiche, a vantaggio di un prodotto molto più costoso, Lucentis, differenziando artificiosamente i due prodotti.

Per il Sistema Sanitario Nazionale l'intesa ha comportato un esborso aggiuntivo stimato in oltre **45 milioni** di euro nel solo 2012, con possibili maggiori costi futuri fino a oltre **600 milioni** di euro l'anno.

Examples of Fines: AGCM – Italy (2014)

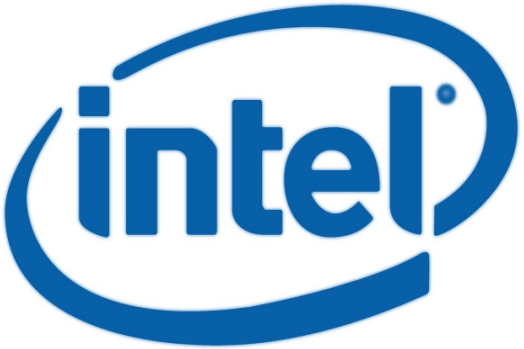


Fine of €180 millions

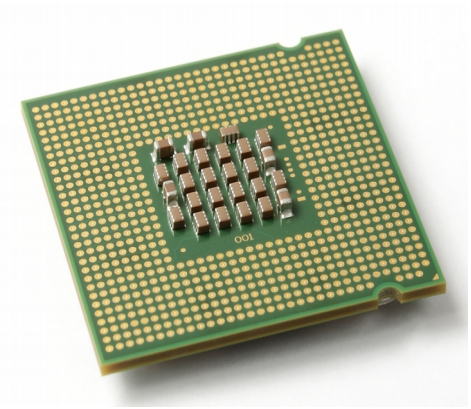
I due gruppi si sono accordati illecitamente per ostacolare la diffusione dell'uso di un farmaco molto economico, Avastin, nella cura della più diffusa patologia della vista tra gli anziani e di altre gravi malattie oculistiche, a vantaggio di un prodotto molto più costoso, Lucentis, differenziando artificiosamente i due prodotti.

Per il Sistema Sanitario Nazionale l'intesa ha comportato un esborso aggiuntivo stimato in oltre **45 milioni** di euro nel solo 2012, con possibili maggiori costi futuri fino a oltre **600 milioni** di euro l'anno.

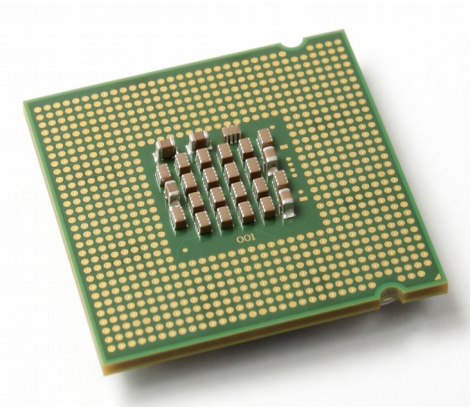
Examples of Fines: DG Comp (2014)



Examples of Fines: DG Comp (2014)



Examples of Fines: DG Comp (2014)

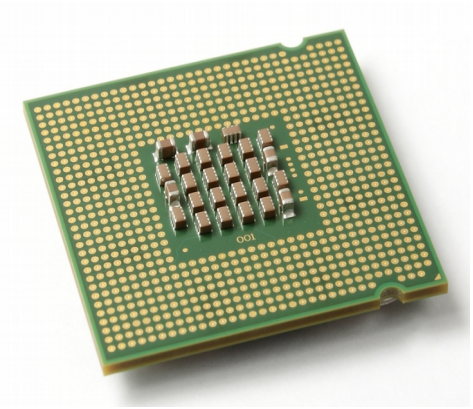


Dominant position in the x86 CPU market

(1) granting rebates to 4 PC and server manufacturers (Dell, HP, NEC, Lenovo) conditional on them obtaining all or almost all of their supplies from Intel, and payments to one downstream computer retailer (Media Markt) conditional on it only selling PCs with Intel CPUs ("conditional rebates"); and

(2) granting direct payments to 3 computer manufacturers (HP, Acer and Lenovo) to halt, delay or limit the launch of specific products incorporating chips from Intel's only rival, AMD (so-called "naked restrictions").

Examples of Fines: DG Comp (2014)



Fine of €1.06 billion

Dominant position in the x86 CPU market

(1) granting rebates to 4 PC and server manufacturers (Dell, HP, NEC, Lenovo) conditional on them obtaining all or almost all of their supplies from Intel, and payments to one downstream computer retailer (Media Markt) conditional on it only selling PCs with Intel CPUs ("conditional rebates"); and

(2) granting direct payments to 3 computer manufacturers (HP, Acer and Lenovo) to halt, delay or limit the launch of specific products incorporating chips from Intel's only rival, AMD (so-called "naked restrictions").

International Context of the Project

- European Competition Network (ECN)
- In 2010 the ECN Forensic IT (FIT) WG was formally established (informal meetings held since 2003)
  - A forum for the European competition authorities helping them to solve technical, procedural and legal issues
- A number of important initiatives have been undertaken:
  - First training programme (March 2009 – March 2010)
    - Forty-four (44) officials belonging to 25 European competition authorities representing 23 different countries
  - EATEP_FIT (Sep 2011 – Aug 2014)
    - Training and exchange programme (September 2011 – August 2014)
    - 125 officers (56 FIT experts and 69 case-handlers) have attended the courses.
    - 52 exchanges have taken place, some of them providing cross-border FIT assistance in dawn raids
  - **EAFIT_TOOLS**

The EAFIT_TOOLS Project

- European project with financial support from the Prevention of and Fight against Crime Programme of the European Union - European Commission - Directorate - General Home Affairs
- **Funding Programme**: Prevention of and Fight against Crime
- **Coordinator**: Italian Competition Authority – AGCM – Dott. Mauro La Noce
- **Scientific Coordination:** Roberto Di Pietro
- **Total Funding**: €710.080,39
- **Period**: November 2013 – October 2015

Partners

AGCM
AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

BWB
BUNDESWETTBEWERBSB

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

KONKURRENCE- OG FORBRUGERSTYRELSEN

CNMC COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA

RÉPUBLIQUE FRANÇAISE
Autorité de la concurrence

REPUBLIC OF ESTONIA
COMPETITION AUTHORITY

ROMA TRE
UNIVERSITÀ DEGLI STUDI

KKV Finnish Competition and Consumer Authority

Hungarian Competition Authority

Authority for Consumers & Markets

KONKURENCES PADOME

Bundeskartellamt

AUTORIDADE DA CONCORRÊNCIA

ROMANIA
CONSILIUL CONCURENTEI

CMA
Competition & Markets Authority

Partners

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

KONKURRENCE- OG FORBRUGERSTYRELSEN

COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA

RÉPUBLIQUE FRANÇAISE
Autorité de la concurrence

Finnish Competition and Consumer Authority

KONKURENCES PADOME

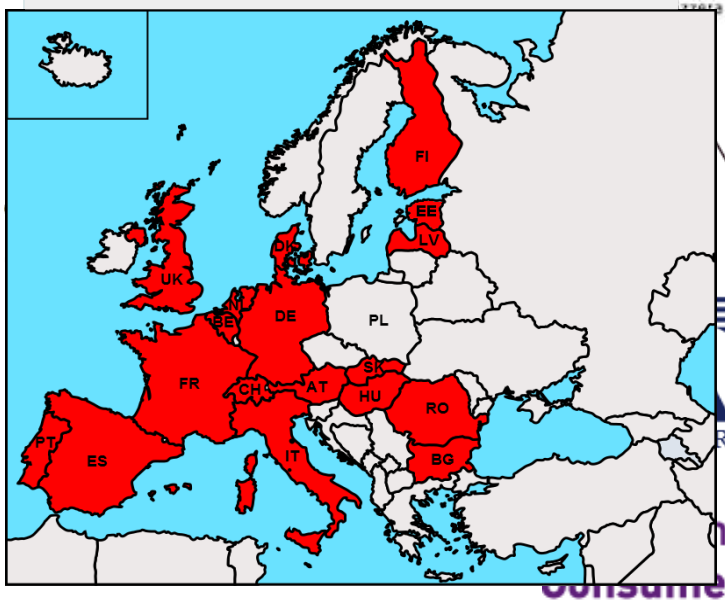
Bundeskartellamt

AUTORIDADE DA CONCORRÊNCIA

ROMANIA CONSILIUL CONCURENTEI

CMA
Competition & Markets Authority

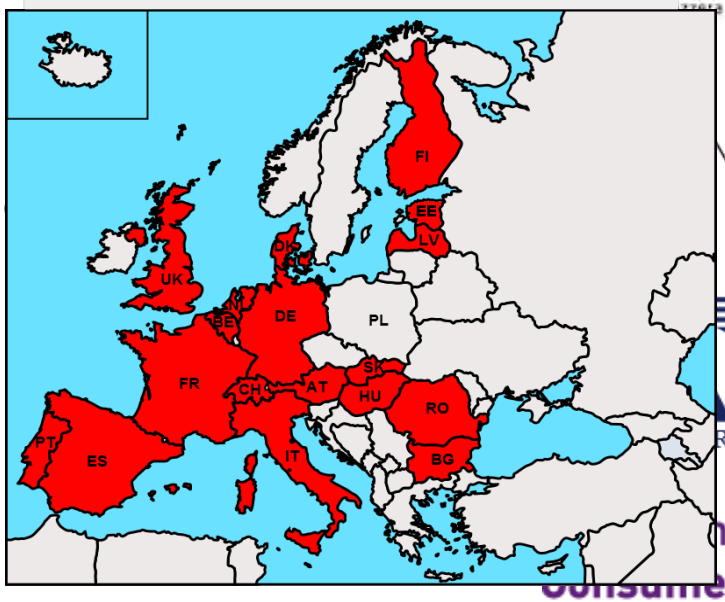
Partners



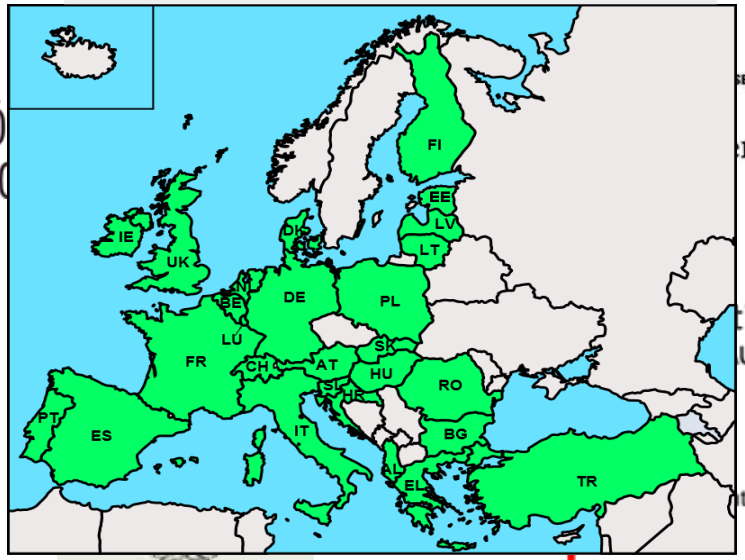
Partners

AGCM
AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

Partners



Stakeholders



AUTORIDADE DA CONCORRÊNCIA

ROMANIA CONSILIUL CONCURENTEI

CMA Competition & Markets Authority

EAFIT_TOOLS Project Objectives

- To boost the technical convergence of tools, protocols and procedures for forensic analysis in the ECN.
  - Collect a set of widely shared requirements about the forensics activities and procedures on cartels investigation and antitrust enforcement of the European Competition Authorities (CAs).
  - To recognize and classify already exiting tools in order to create a map between the CAs requirements and the existing open-source libraries and tools.
  - To integrate the selected open-source tools and develop a prototype of an European Antitrust Forensic IT software.
- Focus on Open source software

Project Phases

- Phase 1: Requirements analysis
- Phase 2: Open Source tools recognition and classification
- Phase 3: Implementation, Testing and User Training

Requirement Analysis

- Elicitation
  - On site interviews
    - 7 Competition Authorities have been visited
  - Requirements workshop
    - 42 attendees from 27 national and transnational Competition Autorities - 2 days
    - Result: 155 raw requirements
- Specification
- Validation

Peculiarities of Antitrust investigations

Peculiarities of Antitrust investigations

1. PRE DAWN RAID
   - Raid preparation (intelligence phase, keywords elicitation, team compositions, etc.)
   - OSInt

Peculiarities of Antitrust investigations

1. PRE DAWN RAID
   - Raid preparation (intelligence phase, keywords elicitation, team compositions, etc.)
   - OSInt

2. DAWN RAID
   - 1 or 2 days on-site for most of the Antitrusts
   - On average 5 to 10 sites investigated at the same time
   - They try to bring home only relevant evidence (no disk images when possible)
   - Interesting artifacts:
     Office documents, pdf, etc... (content and metadata)
     Deleted files
     Emails (also from mail servers)
     Backups, Instant Messaging, Mobile phones
   - FIT activities most of time end with the dawn raid
   - Wiping

Peculiarities of Antitrust investigations

1. PRE DAWN RAID
   - Raid preparation (intelligence phase, keywords elicitation, team compositions, etc.)
   - OSInt

2. DAWN RAID
   - 1 or 2 days on-site for most of the Antitrusts
   - On average 5 to 10 sites investigated at the same time
   - They try to bring home only relevant evidence (no disk images when possible)
   - Interesting artifacts:
     Office documents, pdf, etc... (content and metadata)
     Deleted files
     Emails (also from mail servers)
     Backups, Instant Messaging, Mobile phones
   - FIT activities most of time end with the dawn raid
   - Wiping

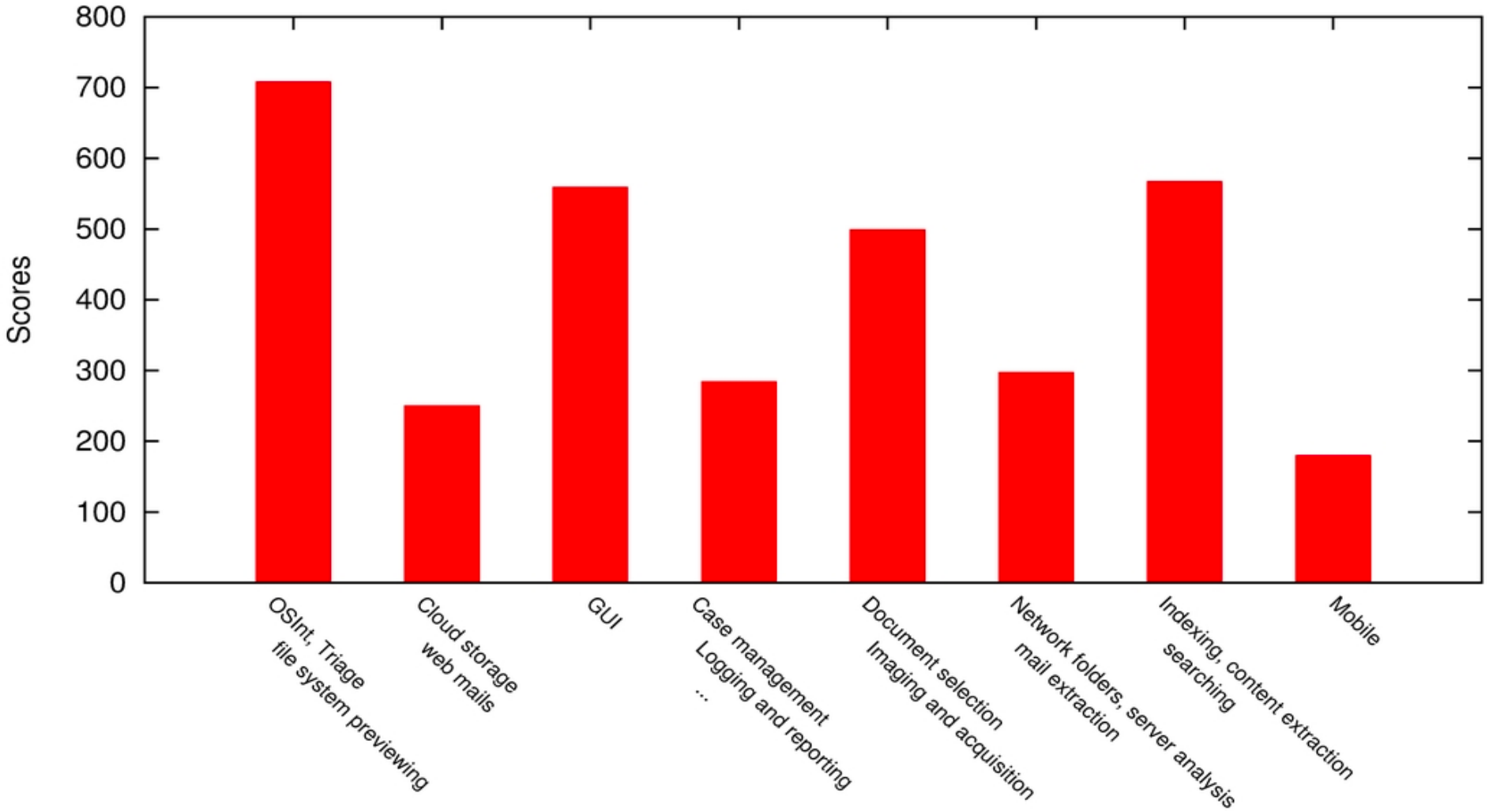
Peculiarities of Antitrust investigations

1. PRE DAWN RAID
   - Raid preparation (intelligence phase, keywords elicitation, team compositions, etc.)
   - OSInt

2. DAWN RAID
   - 1 or 2 days on-site for most of the Antitrusts
   - On average 5 to 10 sites investigated at the same time
   - They try to bring home only relevant evidence (no disk images when possible)
   - Interesting artifacts:
     Office documents, pdf, etc... (content and metadata)
     Deleted files
     Emails (also from mail servers)
     Backups, Instant Messaging, Mobile phones
   - FIT activities most of time end with the dawn raid
   - Wiping

3. POST DAWN RAID
   - Most of the Antitrusts cannot review the collected evidence without the part
   - Only a few have a large infrastructure lab (DK, DE)

Sets of requirements: relevance



The EAFIT_TOOLS Indexing software

- It will be delivered at the end of the project (Oct 2015):
  - Distributed system easy to set-up
  - Indexing of massive amount of documents (parallelizing computation On Site)
  - Team file reviewing
  - Multi user and multi case management
  - Collaborative tagging and labelling
  - Flexible:
    - On site
    - In Lab
  - It will be probably released under GPLv3 licence

The dawn raid use-case scenario

Triage Phase

Analysis Phase (On Site)

The dawn raid use-case scenario

Triage Phase

Analysis Phase (On Site)

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

The dawn raid use-case scenario

Triage Phase

Live Distribution

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

Analysis Phase (On Site)

EAFIT_TOOLS Software

The dawn raid use-case scenario

Triage Phase

Live Distribution

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

Analysis Phase (On Site)

EAFIT_TOOLS Software

The dawn raid use-case scenario

Triage Phase

Live Distribution

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

Analysis Phase (On Site)

EAFIT_TOOLS Software

The dawn raid use-case scenario

Triage Phase

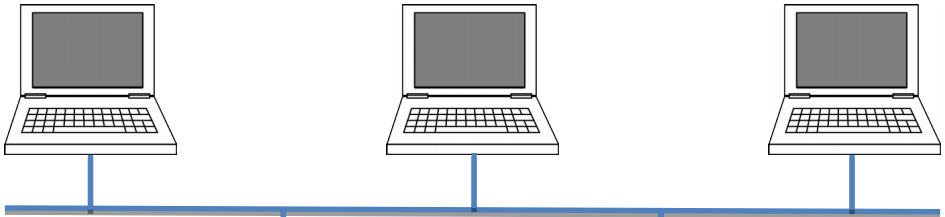
Live Distribution

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

Analysis Phase (On Site)

EAFIT_TOOLS Software



Case
Handler

Case
Handler

Case
Handler

The dawn raid use-case scenario

Triage Phase

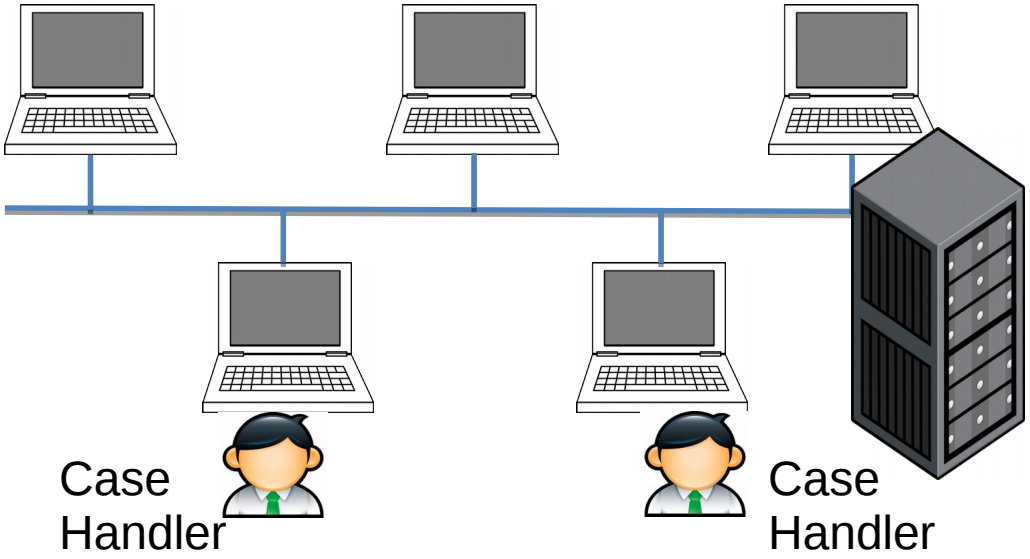
Live Distribution

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

Analysis Phase (On Site)

EAFIT_TOOLS Software



The dawn raid use-case scenario

Triage Phase

Live Distribution

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

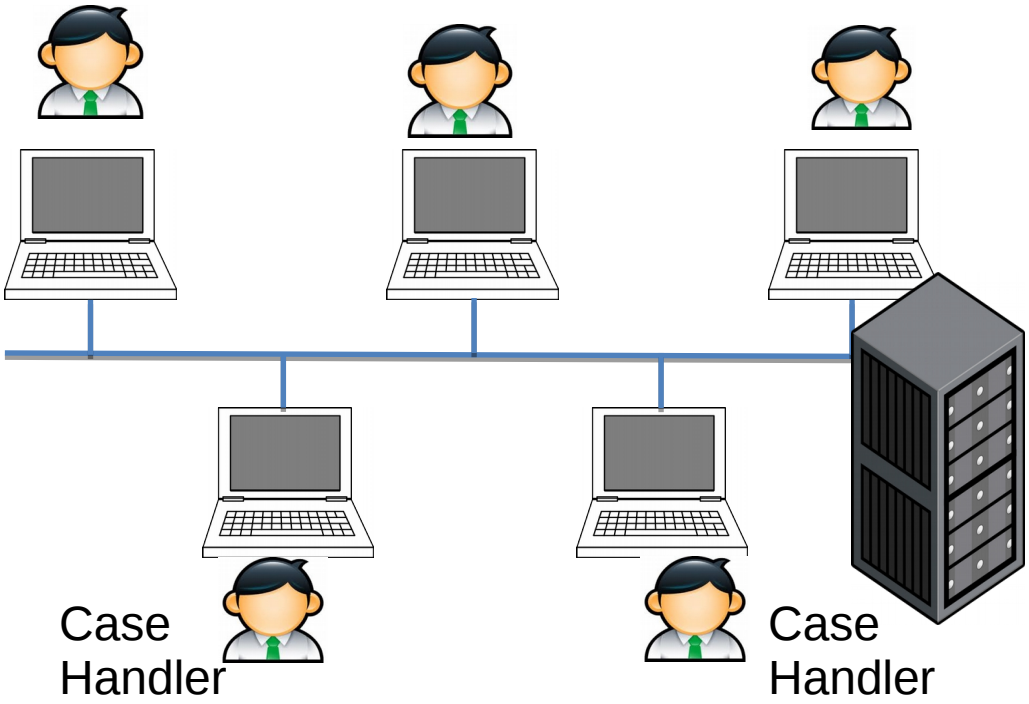
Analysis Phase (On Site)

EAFIT_TOOLS Software

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

Case
Handler



Case
Handler

Case
Handler

The dawn raid use-case scenario

Triage Phase

Live Distribution

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

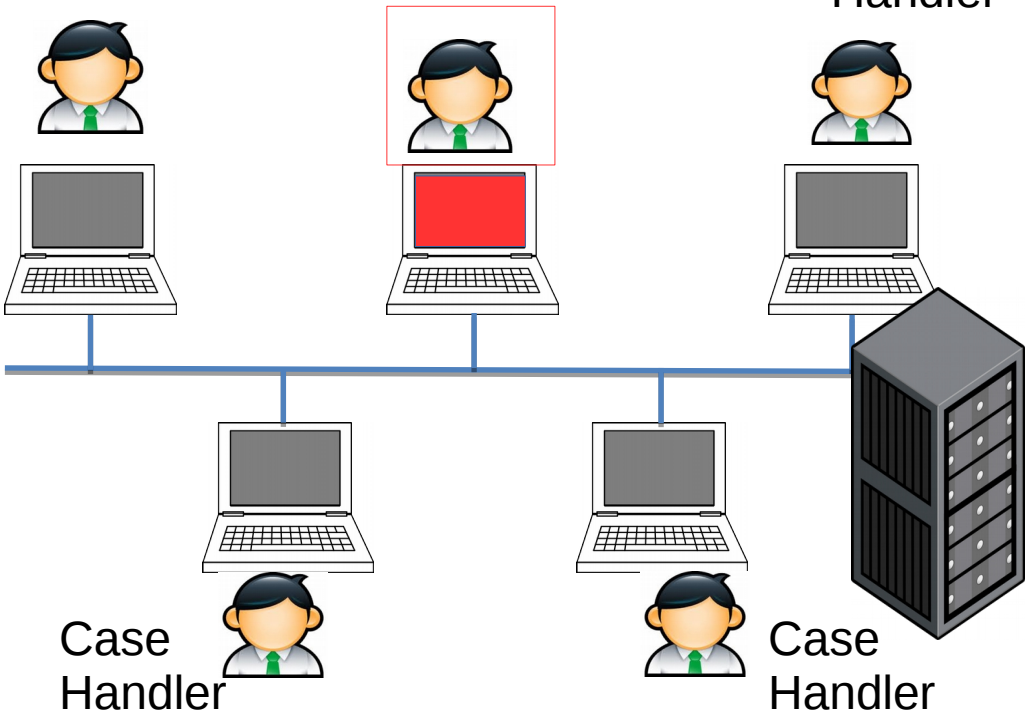
Analysis Phase (On Site)

EAFIT_TOOLS Software

Case Handler
Fit Expert 2

Administrator
Fit Expert 1

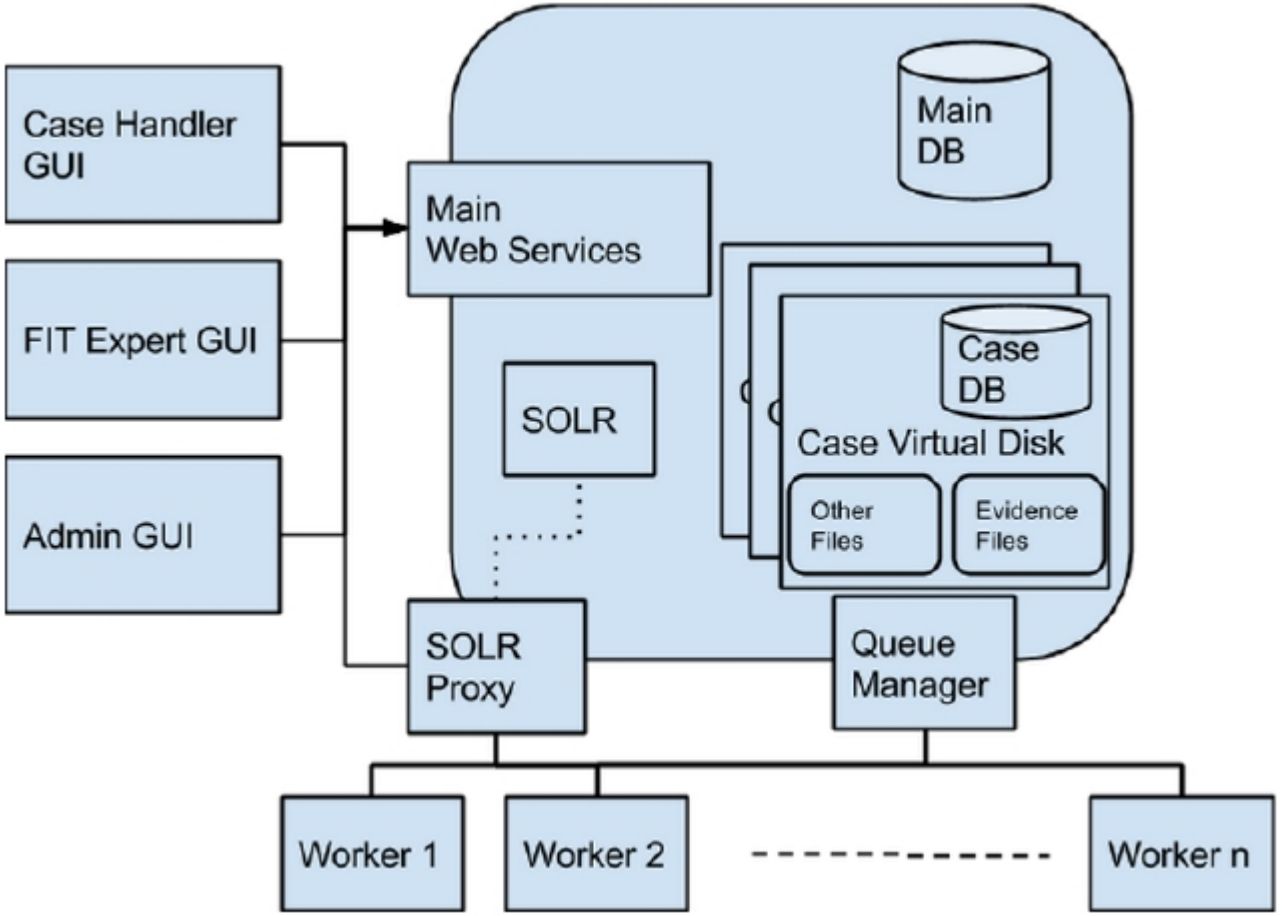
Case
Handler



Case
Handler

Case
Handler

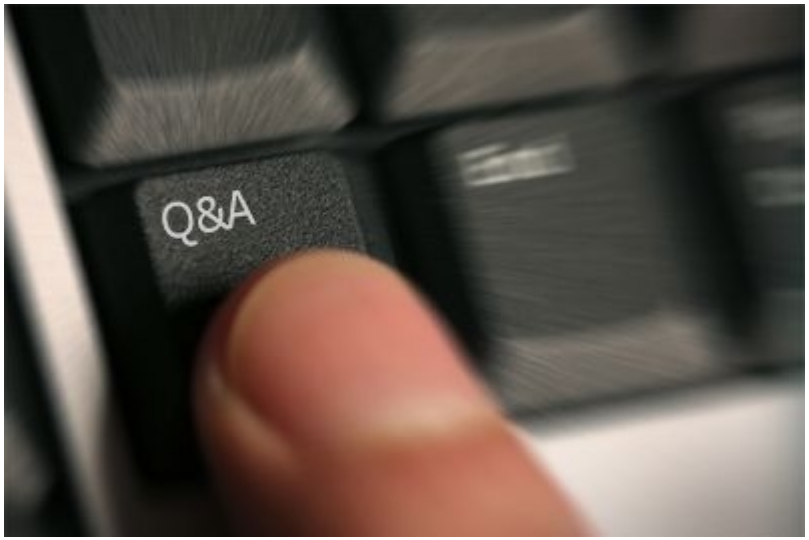
The EAFIT_TOOLS Indexing software: the architecture



Final remarks

- Forensic IT areas are rapidly expanding and Antitrust investigations are a clear example
- Forensic collection of artifacts + On Site Indexing of a large amount of data + collaborative reviewing is a MUST for them
- OSInt is another point of attention
  - i.e.: Recover info about outsourced services before dawnraid
- The european antitrust strategy: Open Source!

* Responsibility for the information and views expressed in this presentation lies entirely with the author.



Presentazione del master in “**Cybercrime e Informatica forense**”

- **Quando**: 28/4/2015 ore 16-19
- **Dove**: Aula alfa, via Salaria 113