European Commission
Directorate-General Home Affairs
Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme

HOME/2009/CIPS/AG/C2-050

i-Code: Real-time Malicious Code Identification

D5.2: Final Management Report

Workpackage:	WP5: Project Management
Contractual delivery date:	June 2012
Actual delivery date:	July 2012
Leading partner:	FORTH
Editor:	Evangelos Markatos
Contributors:	all partners

Executive Summary:

In this deliverable we present the management report of the second year of the i-Code project. Overall, the project progressed well and achieved its objectives. All deliverables for this period have been delivered and the final workshop has been completed. The developed tools have been integrated into the project's console which has been operational for months. The partners have also published several papers in prestigious conferences and journals as can be seen at http://www.icode-project.eu/publications/

With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme.
European Commission - Directorate-General Home Affairs

This project has been funded with the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Commission - Directorate-General Home Affairs. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

1 Publishable Summary

1.1 Summary of project objectives

The objectives of this project are: (i) to design and prototype a system for network-level real-time detection of malicious code spread, (ii) to customize and provide a malware infrastructure which will aid users to categorize and identify captured malware, (iii) to facilitate the detection of malware in high-speed next-generation networks through the design and prototyping of novel execution architectures, and (iv) to maximize the impact of the project through aggressive and effective dissemination of the project's results.

1.2 Work performed and results achieved

During the second year of the project, the individual tools were implemented and integrated into a console. The console has been operational for several weeks and had intercepted several instances of network-based malicious code. All deliverables have been delivered and the final workshop of the project has been successfully organized.

1.3 Project web site

The web site of the project featuring all the public and dissemination information can be reached at http://www.icode-project.eu

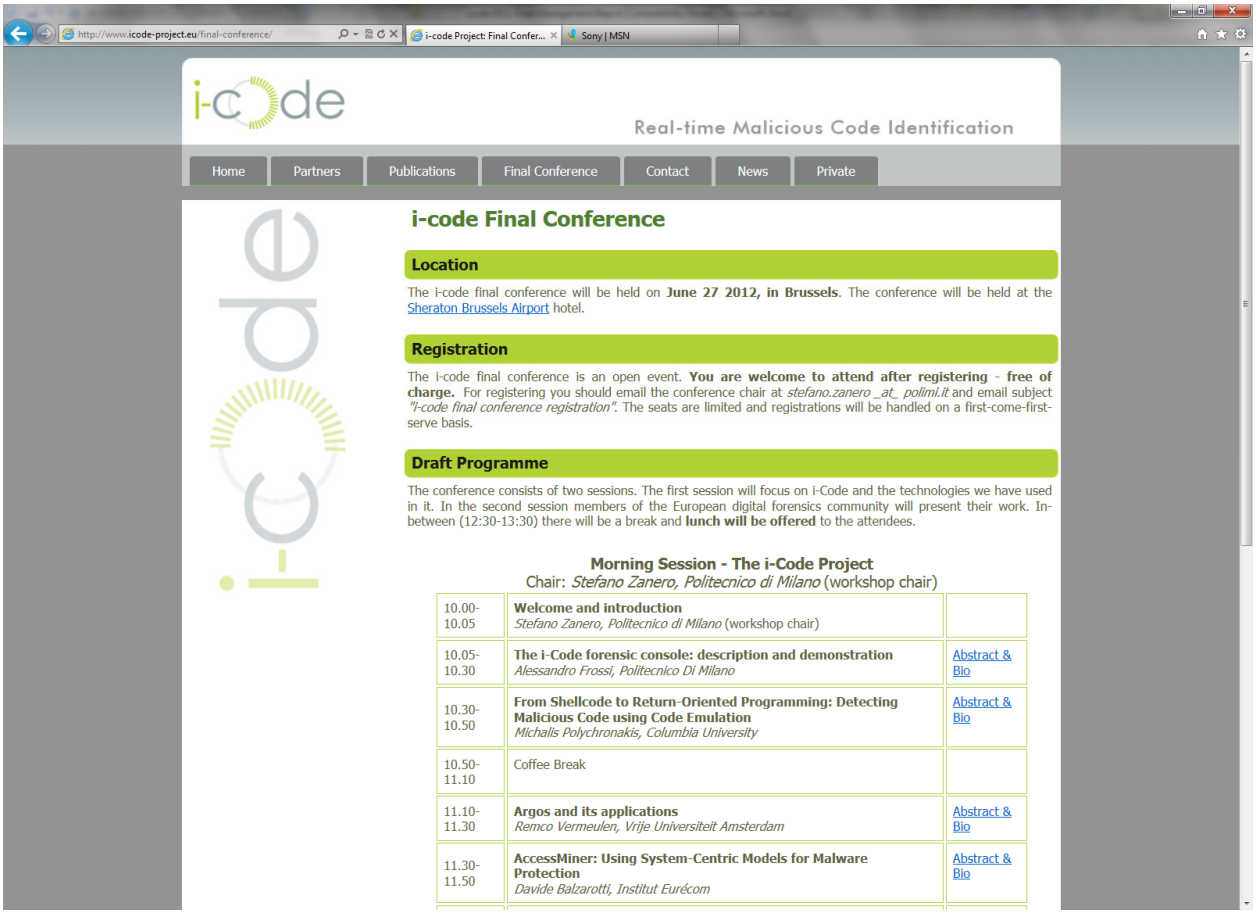

Figure 1: Screenshot of the website of the project. In this screenshot we see the program of the final workshop of the project.

2 Project Objectives, work Progress and Achievements, Project management

2.1 Project Objectives for the period

The main objectives for the reporting period are: (i) to customize and provide a malware infrastructure which will aid users to categorize and identify captured malware, (ii) to facilitate the detection of malware in high-speed next-generation networks through the prototyping of novel execution architectures, and (iii) to maximize the impact of the project through aggressive and effective dissemination of the project's results.

2.2 Work progress and achievements during the period

The progress of the project per WorkPackage is summarized as follows.

2.2.1 WP2: Implementation

2.2.1.1 Summary of progress towards objectives

The goal of WP2 was to implement the individual detection and analysis components of the i-Code real-time malicious code detection system as proposed in WP1 (Design). In particular, the project partners implemented the following tools and sensors in order to detect and analyze malicious code and Internet attacks in real time:

- Detection of shellcode by network-level emulation (FORTH):
  This sensor executes the payload of network traffic on the fly and verifies whether or not it contains malicious code.

- Detection of malware on the end host (EURECOM):
  This sensor detects malware by detecting deviations from the normal behavior of applications that are likely caused by malware.

- A scalable, high-performance I/O architecture to speed up payload execution (VU):
  This tool speeds up network-based intrusion detection by reducing the OS bottlenecks in accessing and processing network traffic.

- Behavioral analysis and classification of shellcode (TUV):
  This tool receives shellcode detected by other sensors and executes it in a sandbox. The resulting decrypted and unpacked shellcode is then fed into a clustering algorithm that checks if the shellcode is entirely new or similar to already analyzed shellcodes.

- i-Code Console (PoliMi):
  The i-Code Console interconnects the aforementioned tools and presents the relevant events in an understandable and usable way.

All components are implemented as proposed in WP1: Design and ready for integration and pilot operation.

2.2.1.2 Highlight clearly significant results

All components are implemented as proposed in WP1: Design and ready for integration and pilot operation.

2.2.1.3 Deviations from the plan and their impact

There were no deviations from the plan.

2.2.1.4 Reasons for failing to achieve critical objectives, if applicable

N/A

2.2.1.5 Use of resources

Figure 2 shows the number of person months invested in WP2 (Implementation) during the second year of the project.

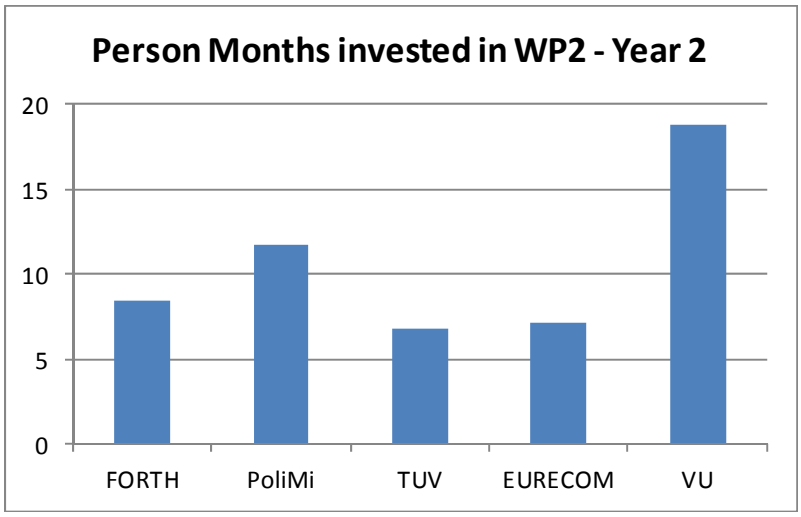

Figure 2: Person Months invested in WP2 during the second year of the project.

2.2.1.6 Corrective actions

No corrective actions were required. WP2 has been completed.

2.2.2 WP3: Integration and Pilot Operation

2.2.2.1 Summary of progress towards objectives

The goal for WP3 was to describe in detail the integration process of all the components described in WP1 (Design) and WP2 (Implementation) into a single system. Each partner took care of completing the implementation of their own tool adding the components that allowed the console to communicate with it:

- Nemu (FORTH):

  This tool was extended with a custom module acting as a client for the Prelude manager and submitting to it all detected events

- AccessMiner (EURECOM):

  A new model enforcement was built and a receiver was created to receive the events from the serial port (where AccessMiner sends them), encode them in the agreed standard for the console and send them to the Prelude manager

- Argos (VU):

  Argos was modified and was set to work as a web proxy server in the testing network; this allowed the tool to analyze all the outgoing requests and detecting possible security threats coming from the Internet

- Anubis (TUV):

  A new shellcode analysis was implemented and the web application was made able to receive automatic submissions directly from a console plugin.

- Console (PoliMi):

  The console was completely implemented and made operational with the events coming from all the tools from the other partners; also, a geolocation plugin, a shellcode submitter plugin and a simple test correlation rule were built and integrated into the system

All the tools were then deployed in a virtual environment that was used to perform the testing phase and the pilot operation: a simple attack scenario was designed and tested and the system reacted very well, detecting all the threats and correctly correlating the information.

In addition, Nemu was deployed in real-world networks to test its effectiveness.

2.2.2.2 Highlight clearly significant results

All the components have been integrated in the i-Code system and their functionalities were successfully tested with real attack scenarios.

2.2.2.3 Deviations from the plan and their impact

There were no deviations from the plan.

2.2.2.4 Reasons for failing to achieve critical objectives, if applicable

N/A

2.2.2.5 Use of resources

Figure 3 shows the number of person months invested in WP3 (Integration and Pilot Operation) during the second year of the project.

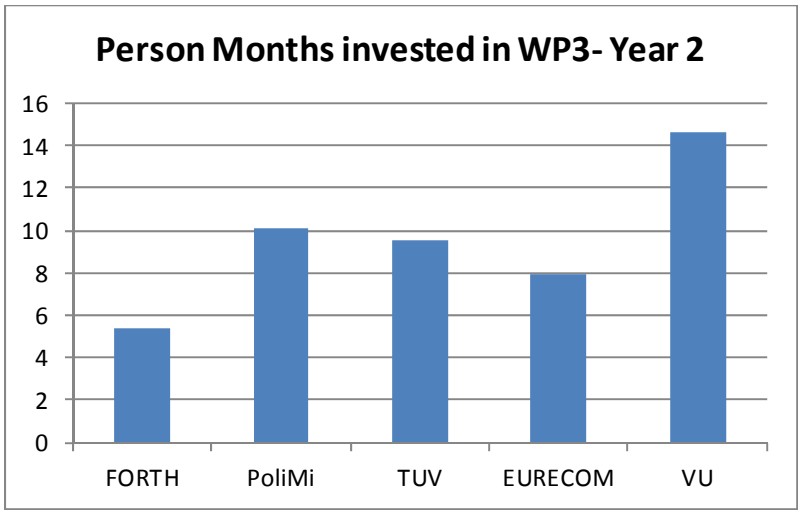

Figure 3: Resources invested in WP3 during the second year of the project.

2.2.2.6 Corrective actions

No corrective actions were required. WP3 has been completed.

2.2.3 WP4: Dissemination

In WP4 we have worked towards the dissemination of the project existence and of its result through various media (most significantly, through scientific, peer reviewed, publications).

2.2.3.1 Summary of progress towards objectives

During the period covered by this report, the i-Code consortium produced a total of 8 papers, all appearing in international conferences with peer-review.

The project website has been active the whole time, collecting all of the public deliverables and the project publications. More than 2,800 users from more than 60 countries have accessed the website, for a total of almost 7,300 pages requested. Most of the accesses are still from Europe and the States.

Our papers were discussed by the media and in few radio and show broadcasts, as well as written articles.

Also, on June 27th, the i-Code final workshop was held in Brussels and all the works made by the partners were presented. In addition, the invited guests delivered some talks about their projects regarding the subject of forensics.

2.2.3.2 Highlight clearly significant results

Our significant result is the fact that the final i-Code workshop was successfully organized and held in Brussels on June 27th. Many people eagerly answered our invitations and were also invited to deliver brief talks on projects they're involved into, regarding the subject of forensics.

2.2.3.3 Deviations from the plan and their impact

None

2.2.3.4 Reasons for failing to achieve critical objectives, if applicable

N/A

2.2.3.5 Use of resources

The following figure provides the number of person months invested in the project per partner.

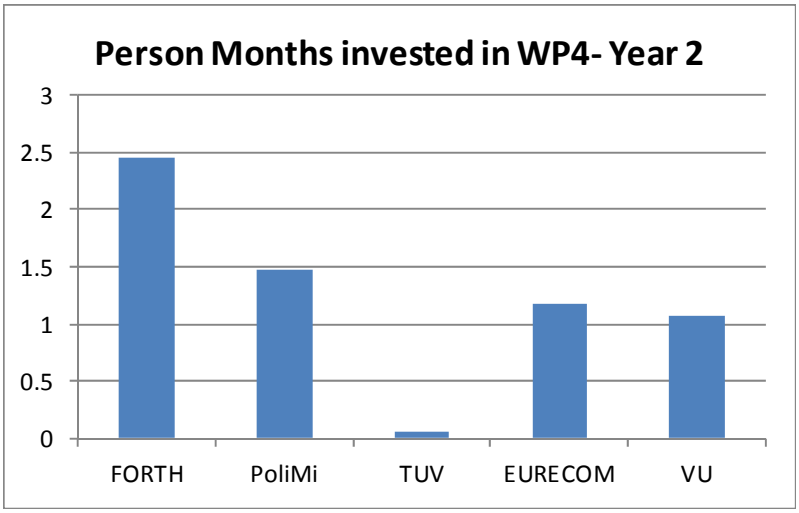

Figure 4: Person months invested in WP4 during the second year of the project.

2.2.3.6 Corrective actions

N/A

2.2.4 WP5: Management

This WorkPackage started at the beginning of the project and lasts for the entire duration of it. To avoid duplication of text, details on the Project Management WorkPackage (WP5) are given in the next section (section 2.3).

2.3 Project Management during the period

2.3.1 Consortium Management tasks and achievements

During the reporting period we successfully completed several management tasks including:

- **Meetings**: We held periodic project plenary meetings which were attended by all partners. The meetings were organized around an agenda circulated well in advance to all partners. During these meetings we discussed the progress of the tasks and scheduled the future work. After the meetings, the coordinator circulated the minutes containing the action points to all partners. During the reporting period we had three plenary meetings and one General Assembly meeting.

- **Collaborative Environment**: we operate on a 24/7 basis a collaborative repository based on SVN. Using this repository, partners can share documents and ideas. We also operate a mailing list for the project and individual mailing lists for the committees.
- **Reporting**. Organized the reporting of the partners on a 6-monthly basis.
- **Liaison**: The coordinator acted as a liaison between the partners and the commission conveying several questions as well as their replies.
- **Amendment**. Coordinated the gathering of all required information and the submission of the information to the Commission so as to implement first amendment of the project's budget.

2.3.2 Problems which have occurred and how they were solved

During the reporting period we did not encounter any problems.

2.3.3 Changes in the Consortium – if any

There were no changes in the consortium.

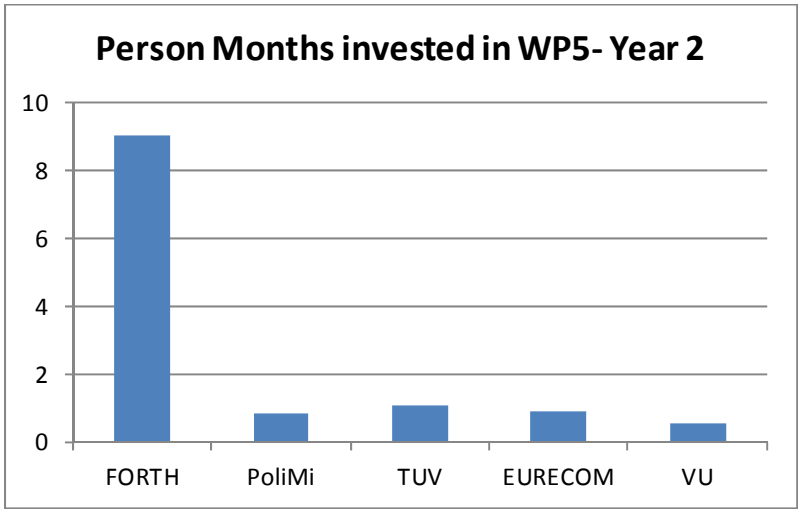

Figure 5: Person Months invested in WP5 during the second year of the project.

Figure 5 shows the person months invested in WP5 (Project Management) during the second year of the project. We see that the project coordinator (FORTH) invested most of the person months, while the rest of the WP leaders invested a small amount of capacity as well.

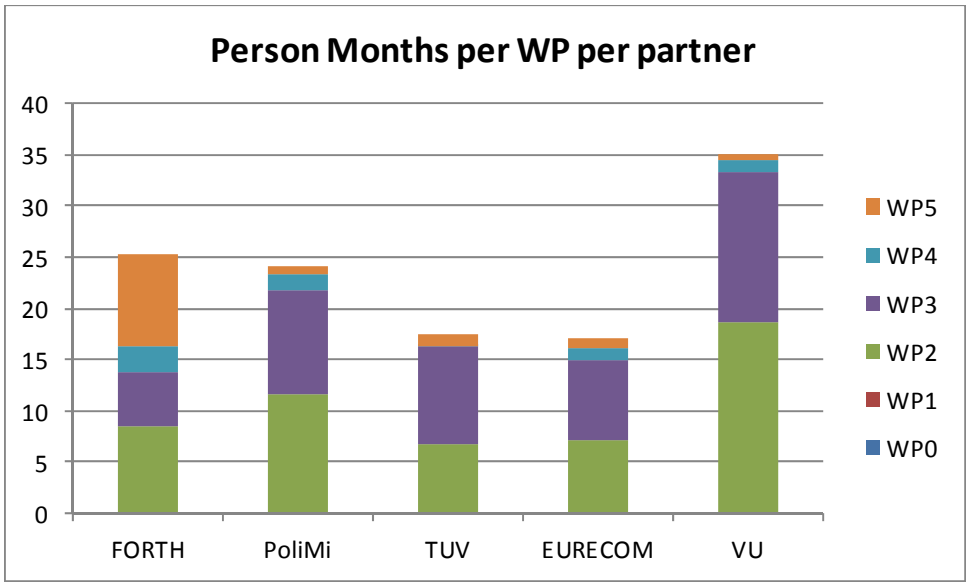

Figure 6: Person Months invested per WorkPackage per Partner during the second year of the project.

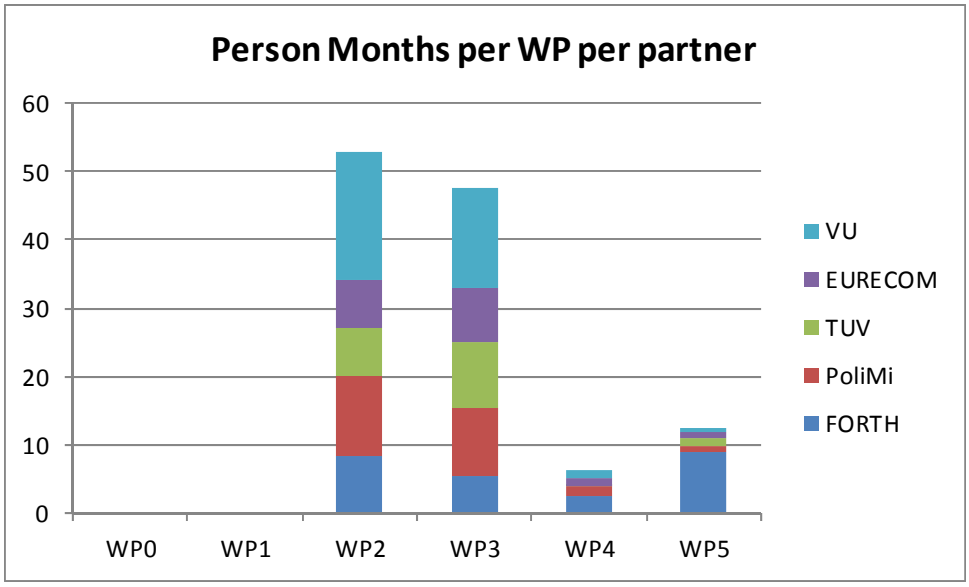

Figure 7: Person Months invested per WorkPackage per Partner. We see that the partners have invested their efforts in WP2 and WP3 which dominate the reporting period. WorkPackages WP4 (dissemination) and WP5 (management) run for the entire duration of the project.

2.3.4 List of project meetings, dates and venues

During the reporting period the following project meetings were held:

- Fourth i-Code plenary meeting, November 10th 2011, Brussels
- Fifth i-Code plenary meeting, March 29th 2012, Milan
- Sixth i-Code plenary meeting, June 6th 2012, Vienna
- Second i-Code GA meeting, June 6th 2012, Vienna
- Final i-Code workshop, June 27th, Brussels

2.3.5 Project Planning and Status

The project has been successfully completed. We expect the partners to continue their work in the area though similar projects, papers, exchanges and collaborations.

2.3.6 Impact of possible deviations from the planned milestones and deliverables, if any

N/A

2.3.7 Any changes in the legal status of the beneficiaries

There were no changes in the legal status of the beneficiaries during the reporting period.

2.3.8 Development of the project website

The web site of the project has been used as the main electronic medium to disseminate information beyond the consortium.

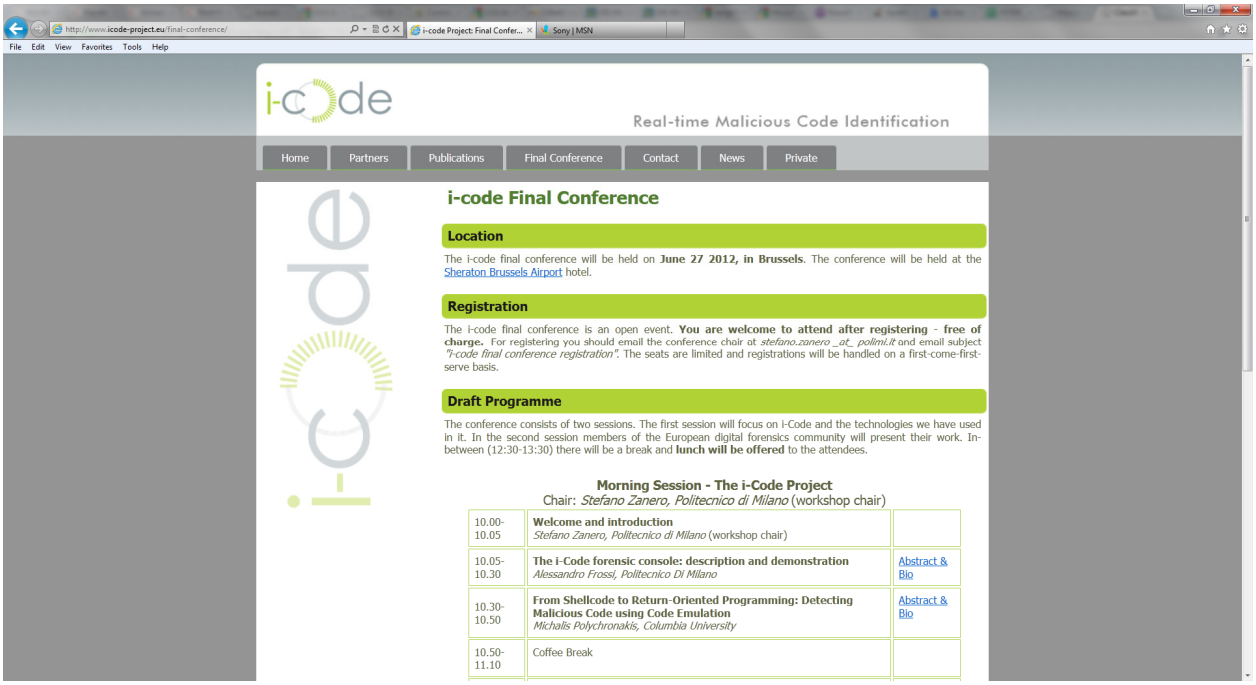

Figure 8: The web site of the project.

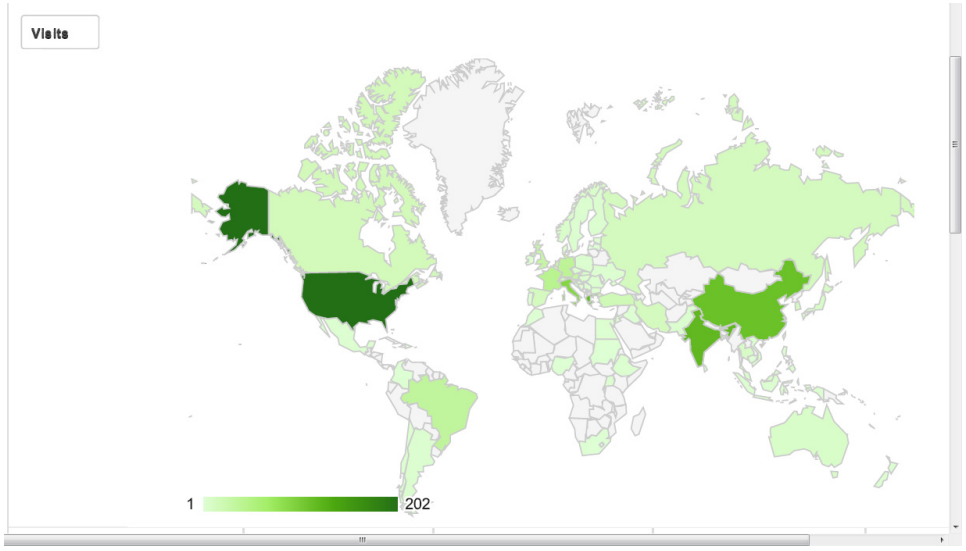

Figure 9: Visitors from more than 73 countries accessed the web site. Interestingly, most of the visits come from countries that are not members of the consortium.

2.4 Deliverables and milestones tables

2.4.1 Deliverables

TABLE 1. DELIVERABLES

Deliverabe no.	Deliverable name	Version	Work Package no.	Lead beneficiary	Nature	Dissemination level[1]	Delivery date from Annex I (project month)	Actual/Forecast delivery date (project month)	Status No submitted/Submitted	Contractual Yes/No	Comments
D2	System Implementation	-	WP2	TUV	R	PU	M18	M18	On the web	Yes	-
D3	Integration and Pilot Operation	-	WP3	PoliMi	R	PU	M24	M25	On the web	Yes	-
D4.2	Midterm dissemination Report	-	WP4	PoliMi	R	PU	M24	M25	On the web	Yes	-
D5.2	Final Management Report	-	WP5	FORTH	R	PU	M24	M25	On the web	Yes	-

[1] **PU** = Public

PP = Restricted to other programme participants (including the Commission Services).

RE = Restricted to a group specified by the consortium (including the Commission Services).

CO = Confidential, only for members of the consortium (including the Commission Services).

Make sure that you are using the correct following label when your project has classified deliverables.

EU restricted = Classified with the mention of the classification level restricted "EU Restricted"

EU confidential = Classified with the mention of the classification level confidential " EU Confidential "

EU secret = Classified with the mention of the classification level secret "EU Secret "