1. Basic Information
1.1. CRIS Number: 2003/005-850.01.03
1.2. Title: Improving investigation involving digital evidence
1.3. Sector: Justice and Home Affairs
1.4. Location: Estonia

2. Objectives
2.1. Overall objective(s):
To strengthen the capacity of law-enforcement agencies to fight against organised crime, money laundering, drugs and cybercrime in Estonia.

2.2. Project purpose:
To improve the capacity of investigators of Central Criminal Police and Police Prefectures to find, collect, secure and analyse digital evidence.

2.3. Accession Partnership and NPAA priority
1. Accession Partnership - November 13, 2001: … to strengthen the capacity of law-enforcement agencies to fight against organised crime, money laundering and drugs.

2. NPAA 2002-2003 (chapter 24.4 Police co-operation): ... In order to improve the administrative capacity of the police force the following measures must be taken: … improve the administrative capacity of police officers, including training of liaison officers, English courses for police officers and offering regular in-service training.

3. 2002 Regular Report on Estonia's Progress Towards Accession (chapter 24 Co-operation in the field of justice and home affairs; Overall assessment): ... In terms of implementation the capacity of police forces should be further developed to combat more efficiently specific forms of organised crime such as [...] and new types of crime (financial crime, money laundering and "high-tech" crime).

2.4. Contribution to National Development Plan
N/A

2.5. Cross Border Impact
N/A

3. Description

3.1. Background and justification:
Description of the current situation
According to an internal gap analysis (source: Central Criminal Police IT Crime Unit), there is an urgent need to improve the capacity of law enforcement agencies to handle digital evidence in order to effectively combat organised crime, money laundering, drugs as well as cybercrime. Today we face the situation where almost 50% of Estonian people use computers and the
Internet. Internet is also getting more and more popular amongst criminals as the main communication mean, therefore the digital evidence is becoming more common and more important to investigation efforts, especially in order to fight against organised crime, drugs, high-tech crime and money-laundering in domestic as well as at international level.

The success of an investigation may depend directly on digital evidence. However, there are currently few investigators who can adequately treat this kind of evidence. The routine procedure consists in sending digital evidence (computers, hard disks, compact disks and other data carriers, even SIM cards etc.) to the Forensic Service Center (FSC), which provides the forensic examination of evidence. But in practice less than ¼ of the cases truly require forensic expertise, whereas almost 80% of the cases do not need thorough examination by a qualified IT expert. Every investigator with proper training and equipment should be able to search data carriers for e-mails, documents and other data that are considered to be relevant in the case. Right now we face the situation where expertise is delayed for about 8 months and there are approximately 100 cases still waiting. This is a serious bottleneck for the whole criminal procedure, which considerably slows down the speed of procedure. In addition, the mistreatment (or “none-treatment”) of digital evidence by investigators is responsible of a loss in the quality of criminal procedure.

As an example, when an investigator has to deal with a computer related case, he orders a forensic examination. One problem is that, at this stage, the investigator does not have a clear idea of the nature of information the computer contains, nor of the exact information he looks for. Therefore, the forensic examination order often contains very general questions, difficult to answer or limited compared to the information available in the computer. The forensic examination expert has of course the possibility to add questions of his/her own but, as a general rule, he/she does not have enough information on the nature and stage of the specific case to do so. The content of the examination ruling cannot contain all the necessary information and therefore the expert does not have the ability to judge about the relevance (or the lack of it) of the found information pieces.

The above-mentioned situation has created a trend in computer examinations — many investigators have started doing computer first stage examination themselves. Based on the information found in the computer, they then decide upon the need of a forensic examination.

The result is that, without proper equipment and knowledge, the digital evidence is often being mistreated at the initial stage and therefore cannot be used at court.

Therefore it is of most importance that investigators of any type of criminal cases where digital evidence is involved, are capable to perform the so called first level forensic examination. It would speed up the proceedings involving digital evidence, increase the quality of investigation and decrease the workload of forensic experts (and it would then be possible for them to concentrate on the examinations really demanding expert knowledge). Systematic fight against organised crime and drugs requires an effective and flexible IT forensic system, which enfolds also a continuous training course(s) on digital evidence treatment as part of curriculum in the Public Service Academy (PSA) for the police cadets and for the investigators of the Central Criminal Police (CCP) and Police Prefectures in the need of supplementary training.

Strategy
Efficient fight against organised crime, drugs and money laundering is set as the priority by the Ministry of Internal Affairs (MoIA) in the strategy document “Police Priorities up to the year 2006”. This document foresees the implementation of modern forensic equipment and techniques as well as the necessary training of qualified personnel. The current project is
considered to be the part of that strategy, as it will intensely contribute to the achievement of strategy objectives.

The sub-chapter 4.3.2 Organised crime (chapter 4.3 Fight against crime) of the “Police Priorities up to the year 2006” states: “/…/ In its struggle against organised crime the police shall direct the main attention on detecting, clearing up and investigating crimes against persons as well as crimes bringing large profits, committed by criminal groups and criminal associations (connected with illegal economic and mediatiorial business, money laudering, articles and substances having restrictions in trade, as well as trafficking in human beings). In the nearest years the further fight against drug-related crimes will be the priority of the police activities. The main target is more intensive detecting of elements of the mentioned crimes by carrying out more skilful surveillance activities and using more effectively materials of pre-trial proceedings /…/”

Fight against organised crime and smuggling shall be based on:

- constant improvement of legislative bases and use of possibilities resulting from that by law enforcement authorities;
- improvement of special technical means and forensic systems;
- ensuring sufficient material-technical conditions for surveillance authorities by the state;
- strengthening the economic police;
- active work of executive power structures and activities of commissions convened by different state management institutions;
- continuous improvement of work of law enforcement authorities, training of personnel;
- co-ordinated co-operation of institutions subordinated to special government organisations;
- active international co-operation.

In co-operation with relevant authorities it is necessary to cut down effectively the property base and profits of organised crime. That presumes existence of appropriate investigative means. /…/ It is necessary to support ideas of implementing more effective and modern criminal surveillance and special forensic means /…/.”

Legal framework

The collection of all kind of evidence (incl. digital evidence) is regulated by the Code of Criminal Procedure. All the investigative agencies (incl. Central Criminal Police and Police Prefectures) are authorised to collect and present the digital evidence at court. According to the article 48 of Code of Criminal Procedure all the digital evidence (the data on data carriers) is considered as information that is established by other data recording. The use of digital evidence in criminal procedure has also been approved at the Supreme Court in Estonia.

“Article 48. Classes of evidence
(1) Evidence in a criminal matter is any factual data on the basis of which the preliminary investigator and court ascertain, pursuant to the procedure provided by law, the existence or absence of an act punishable pursuant to criminal procedure, the guilt of the person who committed such act, and other facts relevant to the just adjudication of the criminal matter.
(2) Such information shall be established by the testimony of witnesses, victims, suspects, the accused or accused at trial, by the opinion of experts, physical evidence, the minutes of

---

1 Connected to the overall objective of the current project (point 2.1)
2 Connected to the project purpose as stated (point 2.2, point 3.4 (activities 2, 4, 5 and 6 of the PAA))
3 Connected to the procurement of special equipment by the means of Estonian co – financing (see Annex 4)
4 Connected to the results 3.3.1, 3.3.2, 3.3.3; activities 2, 4, 5 and 6 of PAA and activities of STTE-s as stated in 3.4
investigative activities and acts of court, and other documents, by photograph or film, audio, video or other data recording, documents or things obtained by way of surveillance.

Article 149. Grounds for conduct of inspection
A preliminary investigator shall conduct an inspection of the scene of a criminal offence, a site, space, object, document or body in order to detect evidentiary traces of a criminal offence or other physical evidence, to ascertain and establish the circumstances of a criminal act and other facts relevant to the criminal matter.”

The new Code of Criminal Procedure that will enter into force on 1st of July 2004 has the similar regulation as to the use of digital evidence.

“Article 63. Evidence
(1) “Evidence” means the statements of a suspect, accused or victim, the testimony of a witness, an expert’s opinion, the statements given by an expert upon provision of explanations concerning the expert’s report, physical evidence, the reports on investigative activities, minutes of court sessions and the reports on surveillance activities, and any other documents, photographs, films or other data recordings.
(2) Evidence not listed in subsection (1) of this section may also be used in order to prove the facts relating to a criminal proceeding.

Article 83. Objective of inspection and objects of inspection
(1) The objective of an inspection is to collect information necessary for the adjudication of a criminal matter, detect the evidentiary traces of the criminal offence and confiscate objects which can be used as physical evidence.
(2) The objects of inspection are:
1) a scene of events;
2) a body;
3) a document, any other object or physical evidence;
4) in the case of physical examination, the person and the postal or telegraphic item.”

Although the procedural regulations in Estonia do not mention the term “digital evidence”, it is covered by general rules of handling evidence. Therefore, further specific regulations for the use of digital evidence are not needed a priori.

To ensure proper education for investigators of all types of crime (organised crime, drugs, cybercrime etc) specific training and amendments to the curriculum for police cadets in PSA should be developed to cover handling of digital evidence. Currently there is no specific course in the PSA covering handling of digital evidence, although there are several subjects on criminalistics.

Considering the nature of the project, no NGOs were consulted during the project preparation process. The project aims at institution building at the central government level and the NGOs are not seen as directly benefiting or having a role in the project’s activities.

3.2. Linked activities:

The following home affairs projects were financed under Phare programme in Estonia:

<table>
<thead>
<tr>
<th>Project no</th>
<th>Name</th>
<th>Amount EUR</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES9620</td>
<td>Supply of electro-optical sensors to Estonian Board of</td>
<td>2 000 000</td>
<td>Completed</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
<td>Amount</td>
<td>Status</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>ZZ9704</td>
<td>The Baltic Eastern Border Management Programme</td>
<td>1 700 000</td>
<td>Completed</td>
</tr>
<tr>
<td>ES9905</td>
<td>Developing Police Criminalistics and Forensic Science</td>
<td>2 500 000</td>
<td>Completed</td>
</tr>
<tr>
<td>ES0007-2</td>
<td>Police training and educational system</td>
<td>390 000</td>
<td>Completed</td>
</tr>
<tr>
<td>ES01.04.01</td>
<td>Developing the readiness to implement SIS</td>
<td>1 675 990</td>
<td>Ongoing</td>
</tr>
<tr>
<td>ES01.04.03</td>
<td>Program of information system for criminal investigation and</td>
<td>605 313</td>
<td>Ongoing</td>
</tr>
<tr>
<td></td>
<td>criminal analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003/005-026.05.01</td>
<td>Enhancing border control and development of border surveillance at Estonian Eastern Border</td>
<td>3 324 600</td>
<td></td>
</tr>
<tr>
<td>2003/005-026.05.02</td>
<td>Extension of Estonian Automated Fingerprint Identification System</td>
<td>2 175 000</td>
<td></td>
</tr>
</tbody>
</table>

The current project presents only indirect links with the projects on Police training and educational system and Developing the readiness to implement SIS. These links are indirect as ES0007-2 was aimed at strengthening the whole educational system of the police and did not cover IT sector. The ES01.04.01 project develops only certain databases and does not provide tools for investigation of IT crimes. The ES01.04.03 project, the criminal intelligence project involving training and purchasing of the software (ANACAPA project) concerns only criminal intelligence work of intelligence units and therefore there is no overlapping with the current project.

There are also a couple bilateral projects linked to the current proposal:


Cybercrime Estonian CART development Project $128,050
The goal of this project is to help the MoIA to develop its capacity to combat cybercrime by identifying a cadre of police to be trained and equipped in the model of the Federal Bureau of Investigation (FBI) Computer Analysis Response Team (CART). This project provides developing a classroom at the PSA training centre designated for cybercrime training and exchange of experts between the Estonian CART and FBI CART in Washington, D.C., as well as advanced training of Estonian police’s knowledge and capacity to fight cybercrime. The U.S. Embassy in Tallinn, through the FBI’s Legal Attaché, has already provided Estonian law enforcement authorities with training seminar 07.-11.07.2003 on internet investigation for customs, security police and police officials.

This project concentrates only on cybercrime issues and does not involve training and equipment for forensic examination of digital evidence.

2. In 2002 the CCP received funds (50 000 EUR) from Germany to purchase the most vital
equipment and software for establishing the unit (computers, laptops, special software for cybercrime investigation purposes). It doesn’t provide the capacity to do IT forensic examination.

The equipment to be procured as co-financing under this Phare proposal is complementary to the equipment provided through German project and does not benefit from any other bilateral assistance financing.

3.3. Results:

3.3.1 System analysis and development plan for the IT Crime Unit composed;
3.3.2 Development of specific adaptations and amendments to the curriculum on handling digital evidence in the PSA for the police cadets and for the investigators of the CCP and Police Prefectures in the need of supplementary training;
3.3.3 Over 200 police officers able to handle digital evidence following specific training.

3.4. Activities:

**Contract 1: Twinning** (12 months, Phare 366 000 EUR + Estonian Co-financing 4000 EUR)

**PAA** (12 working months over 12 consecutive months, cost Phare 180 000 EUR)

Tasks:
1. Analysis of the current situation in Estonia (incl. analysis of the Estonian legislation, administrative capacity and other relevant factors) (1 month).
2. Producing the system analysis and development plan for IT Crime Unit (1-2 months).
3. Making the arrangements necessary to conduct the training courses for investigators and forensic experts (in close co-operation with STTE 1 and 2):
   - Basic training (as a 1 day seminar) – for investigators on search and securing digital evidence on the crime scene as well as on elementary analysis of the evidence. The target group consists of 200 investigators from Police Prefectures dealing with digital evidence on the scene (4 groups each 50 persons) (2 months);
   - Advanced training (2-3 days) – for investigators on copying data carriers, examining and analysing them (searching for files, recovering erased files, presenting the results) with the forensic program that is to be procured from co-financing funds in the framework of the current project. The target group consists of 40 investigators from Police Prefectures and CCP (1 month);
   - Expert level training (5 days) – for 5 investigators of the IT Crime Unit and 2-3 forensic experts on in-depth training on the use of the software (1 month).
4. Making the arrangements necessary to compile, translate and publish the elementary guide (approximately 300 exemplars) for investigators handling digital evidence on the scene (consisting of basic information and first step instructions on the crime scene investigation where digital evidence is involved) (1 month). This publication should be relatively short, easily readable and understandable (with visual images), pocket sized (foldable) for convenient use by investigators;
5. Making the arrangements necessary to compile, translate and publish the practical handbook for cybercrime investigators and other investigators dealing with digital evidence. The purpose of the handbook is to compile the most reliable and relevant information together in one publication as the information on cybercrime investigation and

---

5 For the indicators please see Annex 1 - Logical Framework Matrix.
digital evidence handling found in libraries and Internet is very scattered and often obsolete or misleading. The handbook should be based on the copy of the free manual issued by Interpol and adapted to local circumstances and legislation. It should contain case studies as the illustration for the subject. The target group is cybercrime investigators as well as forensic examiners (approximately 60 items) (2 months);

6. In co-operation with STTE-s development of the specific curriculum for the PSA on the cybercrime investigation and IT forensic. The target group of the training programme(s) are the cadets of the PSA and investigators of the CCP and Police Prefectures in the need of supplementary training. (1-2 months)

Profile:
- Higher education in the corresponding field (police or law);
- Previous experience in a Member State in establishing similar units for law enforcement;
- Knowledge on cybercrime investigation;
- Knowledge on compiling and conducting training programmes;
- Good communications skills;
- Computer literate;
- Fluency in spoken and written English.

**PAA assistant** (12 working months over 12 consecutive months, cost Phare 12 000 EUR)

Tasks:
- Provision of full time assistance for purposes of translation and interpretation, organisation of meetings and other office duties on a daily basis.

**MS Project Leader** (for 20 working days over 12 consecutive months, cost Phare 26 640 EUR)

Tasks:
- Co-ordination and supervision of the project (incl. 5 working days per quarter in Estonia during the implementation of the project);
- Composition of the reports.

Profile:
- Long-term experience with investigations in a Member State involving digital evidence
- Excellent leadership quality and communication skills;
- Fluency in spoken and written English;
- Computer literate.

**EU STE 1** (150 days over 6 months, Phare 61 160 EUR) and **EU STE 2** (150 days over 6 months, Phare 61 160 EUR)

Tasks (in close co-operation with the PAA):
- Conducting training needs analysis of all the above-mentioned target groups (2 weeks);
- Preparing and conducting the basic training (as a 1 day seminar) – for investigators on search and securing digital evidence on the crime scene as well as on elementary analysis of the evidence. The target group consists of 200 investigators from Police Prefectures dealing with digital evidence on the scene (4 groups each 50 persons) (1-2 months);
- Preparing and conducting the advanced training course (2-3 days) for investigators on copying data carriers, examining and analysing them (searching for files, recovering erased
files, presenting the results) with the forensic program that is to be procured for co-financing funds in the framework of the current project. The target group consists of 40 investigators from Police Prefectures and CCP (1 month).

- Preparing and conducting the expert level training (5 days) for 5 persons from the IT Crime Unit in CCP and 2-3 forensic experts from FSC on practical investigation of IT-crimes and in-depth training on the use of the software (1 month).
- Assistance to the PAA in compiling training materials, elementary guide and handbook (1-2 months).
- Developing the curriculum for the PSA on the cybercrime investigation and IT forensic (1-2 months).

Profile STE 1:
- Higher education in the corresponding field (police or law);
- At least 5 years of practical experience as a cybercrime investigator;
- Practical experience in using EnCase software or any equivalent investigation software;
- Experience in compiling and conducting training courses;
- Good communication skills;
- Computer literate;
- Fluency in spoken and written English.

Profile STE 2:
- Higher education in the IT field;
- At least 5 years of practical experience as an IT forensic expert in a Member State;
- In-depth knowledge and practical experience in using EnCase software or any equivalent investigation software;
- Experience in compiling and conducting training courses;
- Good communication skills;
- Fluency in spoken and written English.

The purpose for STE 1 and STE 2 is to have parallel functions to compile and conduct all the training courses as well as provide expert assistance to PAA regarding other tasks in close cooperation. It is important to get the in-depth expertise to the issues from both investigation and forensic viewpoint (see both STE 1 and STE 2 profiles).

Translation and producing training materials (ca 300 elementary guides and ca 60 handbooks) Phare 6 000 EUR, Estonia 4 000 EUR.

Contract 2
Procurement of the necessary software and hardware to the CCP, the Police Prefectures and the PSA is financed from national co-financing (100 000 EUR). For the detailed list of the items being purchased see annex 4.

3.5 Lessons learned:

Ministry of Internal Affairs is currently implementing four Phare projects: Developing the readiness to implement SIS, Program of information system for criminal investigation, Enhancing border control and development of border surveillance at Estonian Eastern border and Extension of Estonian Automated Fingerprint Identification system. All projects cover different fields of justice and home affairs.

As regards project implementation the decentralised approach has been most successful. Direct
beneficiaries are implementing the projects having designated or employed project managers and assisting staff for proper implementation. The current project will be implemented by CCP. The project requires close involvement of the MoIA as CCP has very little experience in Phare projects. Persons who participated in elaboration of project application will also be involved during implementation phase.

On the basis of the experience acquired from the implementation of previous twinning project (ES0007-2), the sub-chapter V.4. (Reflections on Implementation; Problems, Modifications and Delays) of the Monitoring Report M/ES/JHA/03005 states: ... Too ambitious project fiche is a lesson learned for the future. In the future Estonian side should also show initiative in composing a TC [Twinning Covenant].

To ensure smooth preparation of the TC the beneficiary (CCP) is showing its best intentions by appointing a twinning counterpart. All directly and indirectly involved institutions are involved in the Steering Committee. Twice a year also gathers the Phare Sectoral Monitoring Working Group on Justice and Home Affairs. The Steering Committee will be set up early on in the project implementation, i.e. within 3 months of signature of the FM.

4. Institutional Framework

Central Criminal Police (CCP)
The CCP is acting under the supervision of the MoIA within the administrative area of Estonian Police Board. The CCP prevents, combats and detects criminal offences which cover the whole state or at least several counties, are very serious, draw major public attention or have had serious consequences. For example:

- serious crimes against persons
- crimes causing great material damage to the state
- crimes related to money laundering
- crimes needing comprehensive international co-operation
- organised crime and serious drug offences
- serious cybercrime

The CCP also co-ordinates the criminal police work at regional level (Police Prefectures).

- There are 4 main departments in the Central Criminal Police: Organised Crime Department, Drug Crime Department, Economic Crime Department and IT Crime Division. Each department combats (corresponding type of) crime at national level and co-ordinates the criminal police work at regional level (Police Prefectures).

Forensic Service Centre (FSC)
The FSC is acting under the supervision of the MoIA within the administrative area of Estonian Police Board. FSC provides forensic expertise and technical assistance for police agencies, the forensic experts participate in pre-trial and court investigative activities as the expert witnesses. As the future of the institution remains uncertain for some time (whether it will remain separate institution or will be merged into CCP) the FSC involvement in the project is limited to IT experts participating in expert forensic training courses. These experts will remain dealing with digital evidence in the future even in case of modification of the FSC structure.

Police Prefectures
Acting under the supervision of the MoIA within the administrative area of Estonian Police
Board. There are 17 regional Police Prefectures (since 2004 there will be 4 large prefectures), each serving one county or a town. A Police Prefecture maintains public order and ensures internal security within its area, prevents, combats and detects criminal and administrative offences, carries out pre-trial investigations in criminal matters in local level and proceeds administrative offences. The criminal police work is being co-ordinated by the CCP.

The investigators participating at the training courses will be selected by the CCP on the proposition of the Police Prefectures taking into consideration their prior experience with digital evidence and their computer skills.

**Public Service Academy (PSA)**
The PSA is acting directly under the MoIA. The PSA is an educational institution providing applied higher education in the field of police work as well as in other fields of administration of the MoIA (tax, customs, correction etc). The PSA will be the central training facility considering the project purpose.

No administrative change is required prior to implementation of the project.

**5. Detailed Budget**

<table>
<thead>
<tr>
<th>Contract 1</th>
<th>Phare Support (EUR)</th>
<th>National Cofinancing</th>
<th>IFT</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twinning package</td>
<td>366 000</td>
<td>366 000</td>
<td>4 000</td>
<td>370 000</td>
</tr>
<tr>
<td>Twinning covenant preparation</td>
<td>7 000</td>
<td>7 000</td>
<td></td>
<td>7 000</td>
</tr>
<tr>
<td>PAA for 12 months</td>
<td>180 000</td>
<td>180 000</td>
<td></td>
<td>180 000</td>
</tr>
<tr>
<td>PAA assistant</td>
<td>12 000</td>
<td>12 000</td>
<td></td>
<td>12 000</td>
</tr>
<tr>
<td>EU MS Project Leader</td>
<td>26 640</td>
<td>26 640</td>
<td></td>
<td>26 640</td>
</tr>
<tr>
<td>EU STE 1</td>
<td>61 160</td>
<td>61 160</td>
<td></td>
<td>61 160</td>
</tr>
<tr>
<td>EU STE 2</td>
<td>61 160</td>
<td>61 160</td>
<td></td>
<td>61 160</td>
</tr>
<tr>
<td>Training materials (ca 300 elementary guides and ca 60 handbooks) (translation and producing)</td>
<td>6 000</td>
<td>6 000</td>
<td>4 000</td>
<td>10 000</td>
</tr>
<tr>
<td>Audit</td>
<td>5 000</td>
<td>5 000</td>
<td></td>
<td>5000</td>
</tr>
<tr>
<td>Reserve (2.5 % max)</td>
<td>7 040</td>
<td>7 040</td>
<td></td>
<td>7040</td>
</tr>
</tbody>
</table>

| Contract 2 | Purchase of hardware (Pentium 4 | 100 000 | 100 000 |
The amounts for co-financing indicated in the table correspond to cash co-financing. In addition, in-kind contributions from the Estonian administration for effective implementation of the twinning/twinning light/TA may be further detailed in the twinning covenant/Terms of references.

Flow and stock data on co-finance will be submitted quarterly for steering committees and to the CFCU and on a half-yearly basis to the Sector Monitoring Working Group. The beneficiary, together with the NAO commits to sound financial management and financial control.

### National co-financing

<table>
<thead>
<tr>
<th>National co-financing</th>
<th>2003</th>
<th>2004</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>State budget</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Translation and publication of training material</td>
<td>4 000</td>
<td>4 000</td>
<td></td>
</tr>
<tr>
<td>Purchase of hardware and software (co-financing)</td>
<td>100 000</td>
<td>100 000</td>
<td></td>
</tr>
<tr>
<td><strong>Total national co-financing</strong></td>
<td>104 000</td>
<td>104 000</td>
<td></td>
</tr>
</tbody>
</table>

The detailed list of the items being purchased is added below (Annex 4). National co-financing will be foreseen under art 23 in State Budget. No bilateral assistance will support national co-financing in the amount indicated in the budget of current project.

### 6. Implementation Arrangements

6.1. Implementing Agency
The Implementing Agency is Central Financing and Contracting Unit (CFCU) within the MoF. The CFCU will be responsible for handling tendering, contracting and payments of contracts.

The responsibility for project preparation, actual implementation and monitoring will remain within the responsibilities of beneficiary institutions.

The Programming Authorising Officer/PAO is:
Mr. Renaldo Mändmets
Deputy Secretary General Ministry of Finance
Phone: (+372) 6 113 545
Fax: (+372) 6 966 810
e-mail: renaldo.mandmets@fin.ee

The Programme Officer/ PO is:
Mr Lauri Tabur  
Deputy Director-General of the Police  
Central Criminal Police  
Phone (+372) 612 3002  
Fax: (+372) 612 3726  
e-mail: lauri.tabur@kkp.pol.ee

A high-level project leader will be nominated before the twinning selection meeting.

The project manager is:  
Mr Alar Must  
Leading Police Inspector  
IT Crime Unit  
Central Criminal Police  
Police Board  
Phone: (+372) 612 3775  
Fax: (+372) 612 3726  
e-mail: alar.must@kkp.pol.ee

A Steering Committee (SC) will be set up to oversee the project implementation. The SC will meet once in a quarter and it will include the representatives of the Police Board, the CCP, the FSC, the PSA, the EC Delegation in Estonia and the MoF. The Steering Committee will meet within 3 months of signature of the FM.

6.2. Twinning  
Direct beneficiaries of the Twinning component are the CCP, Police Prefectures, the PSA and the FSC.

Counterpart for the expert will be:  
Ms. Ulvi Oksa  
Head of Bureau  
Foreign Relations Bureau  
Estonian Police Board  
Phone: (+372) 612 3070  
Fax: (+372) 612 3080  
e-mail: ulvi.oksa@pol.ee

6.3. Non-standard aspects  
No non-standard aspects are foreseen. The Twinning Manual (Preparing Candidate Countries for Accession to the EU. Institution Building. A Reference Manual on “Twinning” Projects) will be strictly followed.

6.4. Contracts  
Twinning—370 000 EUR

7. Implementation Schedule  
7.1. Start of tendering/call for proposals  
October 2003

7.2. Start of project activity  
January 2004
7.3. Project Completion
January 2005

8. Equal Opportunity
During the implementation of the project there will be no discrimination on the grounds of race, sex, sexual orientation, mother tongue, religion, political or other opinion, national or social origin, birth or other status. Equal opportunities for women, men and minorities will be ensured by the Steering Committee during the implementation of the project. The Estonian laws and regulations concerning the equal opportunities for women, men and minorities will strictly be followed. Equal opportunity for men and women to participate in the project will be measured by recording the experts and consultants employed.

9. Environment
N/A

10. Rates of return
N/A

11. Investment criteria
11.1 Sustainability
The sustainability of the training activities will be guaranteed by the contracts to be signed by all participants to the training, which obligate the participants (advanced and expert level training) to compensate the training costs if they decide to quit police work during the first 3 years after completion of the training courses.

The involvement of PSA in the project is guaranteed by the confirmation letter issued by the PSA.

Development of a permanent curriculum in PSA will also ensure sustainability by providing own capacity for future training of police officers in handling of digital evidence.

12. Conditionality and sequencing
Before the training sessions could start, necessary hardware and software is to be procured from co-financing funds (for detailed draft list of the items being purchased see Annex 4).

Sequencing
The elementary guide should also be composed and produced before the basic training. The exact timetable concerning other activities will be provided in the Twinning Covenant.
ANNEXES TO PROJECT FICHE
1. Logical framework matrix in standard format;
2. Detailed implementation chart;
3. Contracting and disbursement schedule by quarter for full duration of programme (including disbursement period);
4. Draft list of the items being purchased for co-financing;
5. Feasibility Studies
## ANNEX 1

### Phare logframe

**LOGFRAME PLANNING MATRIX FOR**

**Project: Improving IT crimes’ investigation**

<table>
<thead>
<tr>
<th>Programme name and number</th>
<th>2003/005-850.01.03</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Contracting period expires:</th>
<th>Disbursement period expires:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Total budget:</th>
<th>Phare budget:</th>
</tr>
</thead>
<tbody>
<tr>
<td>470 000 EUR</td>
<td>366 000 EUR</td>
</tr>
</tbody>
</table>

### Overall objective

To strengthen the capacity of law-enforcement agencies to fight against organised crime, money laundering, drugs and cybercrime

<table>
<thead>
<tr>
<th>Objectively verifiable indicators</th>
<th>Sources of Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vast improvement in the quality and speed of criminal procedure involving digital evidence compared to the previous years: 1) The number of criminal cases involving digital evidence is increased 200% compared to the year 2002, deadline: 2006; 2) The average duration of investigation in cases involving digital evidence is decreased 20% compared to the year 2002, deadline: 2006</td>
<td>Police records and FSC records</td>
</tr>
</tbody>
</table>

### Project purpose

To improve the capacity of investigators of Central Criminal Police and Police Prefectures to find, collect, secure and analyse digital evidence

<table>
<thead>
<tr>
<th>Objectively verifiable indicators</th>
<th>Sources of Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>The workload of IT forensic experts in FSC (number of examinations per expert) is reduced 20% compared to the year 2002, deadline: 2006; More digital evidence involved in criminal procedure:</td>
<td>Police records and FSC records</td>
</tr>
</tbody>
</table>
The number of criminal cases involving digital evidence is increased 200% compared to the year 2002, deadline: 2006; Capacity to react quickly and take effective measures to improve international police co-operation (24/7 network – EC Cybercrime Convention)

<table>
<thead>
<tr>
<th>Results</th>
<th>Objectively verifiable indicators</th>
<th>Sources of Verification</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. System analysis and development plan for the IT Crime Unit composed (3.3.1); 2. Development of specific adaptations and amendments to the curriculum on handling digital evidence in the PSA for the police cadets and for the investigators of the CCP and Police Prefectures in the need of supplementary training (3.3.2); 3. Over 200 police officers able to handle digital evidence following specific training (3.3.3)</td>
<td>1. Both documents exist in written form, deadline: April 2004. 2. Meetings with PSA stuff taken place, recommendations exist in written form, deadline: January 2005. 3.1 200 police officials trained, 300 leaflets issued, deadline: June 2004; 3.2 40 investigators trained, approximately 50 handbooks issued, deadline: July 2004; 3.3 5 persons from IT Crime Division and 2-3 forensic experts from the FSC trained, deadline: August 2004.</td>
<td>Project reports, training records (list of participants etc)</td>
<td>Availability of trainees. Full co-operation of all parties.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activities</th>
<th>Means</th>
<th>Cost (EUR)</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract 1 PAA:</td>
<td>Twinning contract (12 months)</td>
<td>Phare</td>
<td>Estonia</td>
</tr>
</tbody>
</table>
Analysis of the current situation in Estonia;
Producing the system analysis of and development plan for IT Crime Unit;
Making the arrangements necessary to compile, translate and publish the elementary guide and handbook;

Making the arrangements necessary to conduct training courses:
a) basic training (1 day seminar, app. 200 persons);
b) advanced training for investigators (image copying, searching for files, recovering erased files, presenting the results) – for ca 40 person (2-3 months);
c) expert training for cybercrime investigators and forensic experts (app 7-8 persons);
Advising (in co-operation with STEEs) on development of the specific curriculum for the PSA on the cybercrime investigation and IT forensic.

Audit

PAA assistant: Provision of full time assistance for

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
<th>Cost</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twinning covenant preparation</td>
<td>PAA (12 months)</td>
<td>7 000 EUR</td>
<td>available.</td>
</tr>
<tr>
<td></td>
<td>PAA assistant (12 months)</td>
<td>180 000 EUR</td>
<td>Hardware and software procured on time.</td>
</tr>
<tr>
<td></td>
<td>MS project leader (5 days per quarter during the implementation of the project</td>
<td>12 000 EUR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EU STTE 1 (150 days over 6 months)</td>
<td>61 640 EUR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EU STTE 2 (150 days over 6 months)</td>
<td>61 640 EUR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Training materials (ca 300 elementary guides and ca 60 handbooks) (translation and producing)</td>
<td>6 000 EUR</td>
<td>4 000 EUR</td>
</tr>
<tr>
<td></td>
<td>Reserve (2.5%)</td>
<td>7 040 EUR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audit</td>
<td>5 000 EUR</td>
<td></td>
</tr>
<tr>
<td>Purposes of translation and interpretation, organisation of meetings and other office duties on a daily basis.</td>
<td>Total: 366 000 EUR</td>
<td>Total: 4 000 EUR</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
</tbody>
</table>
| **MS Project Leader:**  
Co-ordination and supervision of the project (incl. 5 man-days per month during the implementation of the project in Estonia);  
Composition of the reports. |  |  |
| **EU STTE 1, 2:**  
Conducting training needs analysis of all the target groups;  
Preparing and conducting the basic training (as a 1 day seminar) – for investigators on search and securing digital evidence on the crime scene as well as on elementary analysis of the evidence. The target group consists of 200 investigators from Police Prefectures dealing with digital evidence on the scene (4 groups each 50 persons)  
Preparing and conducting the advanced training course (2-3 days) for investigators on copying data carriers, examining and analysing them (searching for files, recovering erased files, presenting the results) (with programme that |  |  |
is to be procured for co-financing funds in the framework of the current project). The target group consists of 40 investigators.

Preparing and conducting the expert level training (5 days) for 5 investigators of the IT Crime Unit and 2-3 forensic experts directly involved in cyber crime investigation on practical investigation of IT-crimes and in-depth training on the use of the software (is to be procured for co-financing funds in the framework of the current project).

Assistance to the PAA in compiling training materials, elementary guide and handbook and in developing the curriculum for the PSA on the cybercrime investigation and IT forensic.

| Contract 2 procurement of hardware and software |  |  | 100 000 EUR |  | Preconditions | Estonian co-financing funds made available |
## Time Implementation Chart

**Project No:** 2003/005-850.01.03

**Project Title:** Improving IT crimes’ investigation

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contract 1</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Twinning package</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAA for 12 months</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>PAA assistant</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>MS project leader</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>STTE 1</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>STTE 2</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Training materials</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
</tbody>
</table>
Cumulative Contracting Schedule

Project No: 2003/005-850.01.03

**Project Title:** Improving IT crimes’ investigation

<table>
<thead>
<tr>
<th></th>
<th>2004</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>31.03.</td>
<td>30.06.</td>
</tr>
<tr>
<td>Contract 1 Twinning package</td>
<td>366 000</td>
<td>366 000</td>
</tr>
<tr>
<td>TOTAL</td>
<td>366 000</td>
<td>366 000</td>
</tr>
</tbody>
</table>
Cumulative Disbursement Schedule

Project No: 2003/005-850.01.03

Project Title: Improving IT crimes’ investigation

<table>
<thead>
<tr>
<th>Date</th>
<th>2004</th>
<th></th>
<th></th>
<th></th>
<th>2005</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>31.03.</td>
<td>30.06.</td>
<td>30.09.</td>
<td>31.12.</td>
<td>31.03.</td>
<td>30.06.</td>
<td>30.09.</td>
<td>31.12.</td>
</tr>
<tr>
<td>Contract 1</td>
<td>91 500</td>
<td>183 000</td>
<td>274 500</td>
<td>366 000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twinning package</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>91 500</td>
<td>183 000</td>
<td>274 500</td>
<td>366 000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Draft list of the items being purchased for co-financing

**Project No:** 2003/005-850.01.03

**Project Title:** Improving IT crimes’ investigation

<table>
<thead>
<tr>
<th>Item / Description</th>
<th>Amount</th>
<th>Total approximate price in EUR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HARDWARE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miro A1796 F 17” 1600x1200@85Hz (max), 0.25mm, 200MHz, 96kHz</td>
<td>17</td>
<td>2 890.08</td>
</tr>
<tr>
<td>Tigma Wings GWS P4 2400</td>
<td>17</td>
<td>28 210.85</td>
</tr>
<tr>
<td>Processor Intel Pentium 4, 2.6GHz/512kB FC-PGA (kit), Hyperthreading, FSB 800 MHz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motherboard Gigabyte GA-8KNXP Intel 875P, FSB800, Hyper-Threading tugi, ATA133,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6xDDR 400/333Mhz Dual Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAM: 512MB DDRAM 333MHz PC2700</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD: 120GB UltraSATA150, Western Digital X2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video: 64MB ATI Radeon 9000, DDRAM, TV-Out, AGP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Soundcard: 6 channel audio integrated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDE RAID: Promise IDE RAID kontroller 0,1, 0+1 RAID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewire IEE1394 3ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDD: 1,44MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DVD NEC ND-1100 4xW(DVD+R), 2,4xRW(DVD+RW), 16xW(CD), 10xRW(CD), 40xR(CD), 12xR(DVD), internal, IDE, 2MB cache, OEM (without software)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case: Tigma Miditor ATX PC-208, 300W PSU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Võrgukaart: Realtec 8100 10/100 emaplaadile integreeritud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keyboard: Keytronic KT-1000 Black</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mouse:</strong> Logitech Pilot Wheel B69 Optical Black</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Windows XP Pro Eng/ Est, CD, OEM</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tigma Enterprise Server SCSI RAID Dual Xeon 2400</strong></td>
<td>1</td>
<td>3 091,40</td>
</tr>
<tr>
<td><strong>Processor:</strong> 2 items Intel Xeon 2,4GHz / FSB 400MHz 512Kb cache</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Motherboard:</strong> Intel SE7500CW2 ATX, Dual Xeon (VGA+LAN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RAM:</strong> 512MB (2x256MB) DDR DIMM 2100 ECC reg.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Controller:</strong> Adaptec SCSI RAID 2120S, 64bit, Ultra320 SCSI, 64MB Cache</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HDD:</strong> 3x 18,3GB, 10 000rpm, 68pin, Ultra160 SCSI, RAID 5 system</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Video:</strong> 8MB ATI integrated</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FDD:</strong> 1,44MB 3,5&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CD ROM:</strong> NEC 52x IDE</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Võrgukaart:</strong> Intel 82550 10/100 UTP integrated</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Case:</strong> SC5200 Enterprise Server ATX SSI korpus</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Keyboard:</strong> BTC-2001 EST layout, wrist support</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mouse:</strong> Logitech Pilot Wheel S61 + Mouse Pad</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>UPS APC BACK CS 500VA</strong></td>
<td>18</td>
<td>1 725,61</td>
</tr>
<tr>
<td><strong>HD Storage (SCSI, Fiber Optical)</strong></td>
<td>1</td>
<td>19 988,32</td>
</tr>
<tr>
<td><strong>SOFTWARE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Encase Forensic Edition ver4</strong></td>
<td>23</td>
<td>44 098,92</td>
</tr>
</tbody>
</table>
Feasibility studies

Project No: 2003/005-850.01.03

Project Title: Improving IT crimes’ investigation

Considering the purpose of the Phare contribution and the fact that the procurement of investment components is fully covered by national co-financing it is considered not necessary to conduct feasibility studies.