EVIDENCE2e-CODEX

Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe

EVIDENCE2e-CODEX

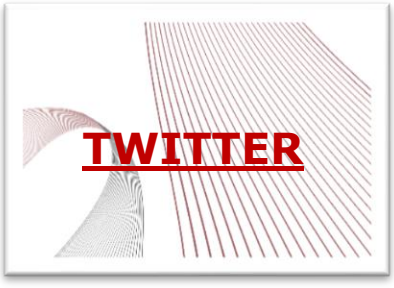
Newsletter #7

15 August 2019 – 14 November 2019

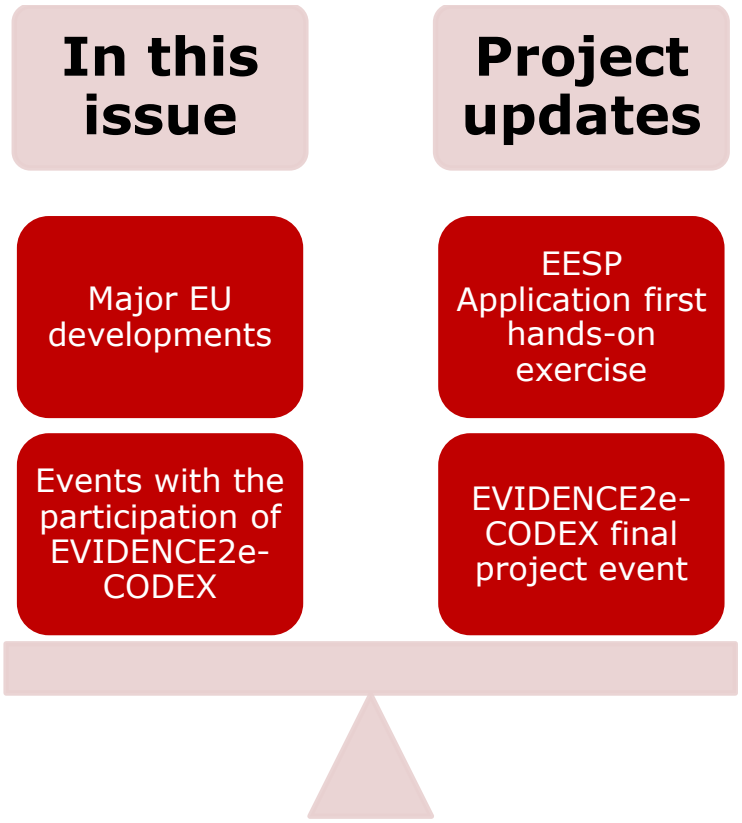
17 Member States, alongside representatives of EUROJUST and EJN, took part in the first hands-on exercise on the Reference Implementation Portal, delivered by the European Commission, and the EVIDENCE2e-CODEX Evidence Exchange Standard Package Application providing feedback and recommendations for improvement of the tools! Check the 7th edition of the EVIDENCE2e-CODEX to learn about this amazing experience!

Dr. Maria Angela Biasiotti, CNR-ISGS, Italy

EVIDENCE2e-CODEX Project Coordinator



This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468



Get in contact

office@evidence2e-codex.eu

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Major EU Developments

Joint Statement on the Launch of EU-U.S. Negotiations to Facilitate Access to Electronic Evidence

Source: European Commission

European Commission and U.S. Department of Justice officials met on 25 September 2019 to begin formal negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations. After a productive first discussion, there was agreement to regular negotiating rounds with the view to concluding an agreement as quickly as possible. Progress will be reviewed at the next EU-U.S. Justice and Home Affairs Ministerial in December 2019.

Background

Electronic evidence is needed in around 85% of criminal investigations, and in two-thirds of these investigations there is a need to obtain evidence from online service providers based in another jurisdiction. Currently, the largest service providers have their headquarters in the United States. The number of requests to the main online service providers continues to increase and grew by 84% in the period 2013-2018.

Cross-border access to electronic evidence has been a regular point on recent EU-U.S. Justice and Home Affairs Ministerial meetings, most recently in Washington on 9 November 2018. The United States and the European Union agree on the importance for both law enforcement and judicial authorities of swift cross-border direct access to electronic evidence, as demonstrated by recent legislation approved or under examination in the United States and the EU.

On 17 April 2018, the Commission proposed to the European Parliament and the Council a Regulation on European Production and Preservation orders for electronic evidence in criminal matters and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings ('e-evidence proposals'). These proposals are currently being discussed by the European Parliament and the Council.

The European Commission proposed on 5 February 2019 to start international negotiations on cross-border access to electronic evidence, necessary to track down dangerous criminals and terrorists. The Justice & Home Affairs Council on 6

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

June 2019 agreed the negotiating directives for the Commission as the European Union's negotiator.

The United States also has a negotiating mandate through the CLOUD (Clarifying Lawful Overseas Use of Data) Act from March 2018, which provides criteria for the negotiation of international agreements to facilitate the ability of other countries partners to obtain electronic data relating to the prevention, detection, investigation or prosecution of serious crime.

More information on cross-border access to electronic evidence can be found here.

LIBE Committee e-Evidence Report Has Been Released

LIBE Committee draft report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters has been released in the beginning of November 2019. The debate on the amendments is expected to continue through the end of December. The final adoption of the report is tentatively scheduled for the beginning of next year.

The full LIBE Committee report can be found here.

During the 'e-Evidence: The Way Forward' workshop held in Brussels at the of September, Ms Birgit Sippel, MEP and Rapporteur for the e-Evidence package, gave an introductory speech about the EU Parliament's view on e-Evidence. Summary of the remarks was published on 6 November 2019 by Prof. Theodore Christakis in the European Law Blog:

Ms Sippel noted that the efficiency arguments put forward by the Commission for the E-Evidence proposal should not override the need to protect fundamental rights.

The EP's criticisms of the e-Evidence proposal include the following:

- *The fact that the criminal laws of the Member States continue to diverge considerably and that the CJEU pointed out problems with current mutual recognition instruments undermine a shift to a system of absolute mutual trust without the involvement of the authority of the enforcing/executing state;*
- *There is a need to reintroduce certain protections into the proposal, including dual criminality which could also help narrow the divergences in the definition of what constitutes a 'serious crime' (the current three-year*

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

threshold would allow for virtually any crime to fall within scope of the European production order);

- *Notification to the data subject is too easily circumvented; therefore, there is a need to ensure in the proposal the ability to inform users about authorities' requests for their data to allow affected persons to exercise their fundamental rights, while at the same time respecting the need to avoid jeopardizing a criminal investigation if based on duly justified confidentiality grounds; in addition, affected persons should be able to bring proceedings before their local court, to guarantee the right to effective remedies and the principle of equality of arms;*
- *Notification to the executing/enforcing state, to enable rejection of a request, is crucial to protecting the rights of individuals; at the same time, notification to the state where the person resides may also be necessary;*
- *The proposal would shift the responsibility for protecting the rights of citizens and residents from Member States to private service providers, which is unacceptable; that said, service providers are important allies that can help ensure the necessity and proportionality of orders as long as they are not solely responsible for this process.*

During Q&A, MEP Sippel cautioned against perceiving EU harmonization as a silver bullet for changing rights-intrusive practices of some Member States, citing the passenger name record (PNR) agreements and directive, which in her opinion resulted in a less protective standard for the EU than previously seen at a national level. Nevertheless, she expressed hope that the Parliament's report will raise the overall protections and close the loopholes in the current draft of the proposal that would allow the law enforcement to use less rights-protective national measures.

Events with the participation of EVIDENCE2e-CODEX

The projects achievements of both legal and technical nature found their way to the EVIDENCE2e-CODEX stakeholders once more via public and closed events around Europe:

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

- **7th Europol-INTERPOL Cybercrime Conference**, 09-11 October 2019, The Hague, the Netherlands

Under the theme 'Law enforcement in a connected future', the three-day event brings together the management of cybercrime units from around the world with partners from academia, international organisations, CERTs and private industry to strengthen cooperation in preventing and combatting cybercrime worldwide. This joint initiative, first held in 2013, alternates every year between Europol's European Cybercrime Centre (EC3) in The Hague and the INTERPOL Global Complex for Innovation in Singapore.

A special session on **constructing the future of cross-border access to electronic evidence** is dedicated to the perfect storm that is the access to electronic evidence nowadays throwing light on the most recent legislative developments and high-level discussions with contributions by: Mr Virgil Spiridon, Head of Operations, Cybercrime Programme Office - Council of Europe; Ms Cathrin Bauer-Bulst, Acting Head of Cybercrime Unit, DG Home - European Commission; and Mr Richard Downing, Deputy Assistant Attorney General, U.S. Department of Justice. EVIDENCE2e-CODEX is honoured to be part of this session, with our two cents on the topic focusing on the practical implementation of the **exchange of cyber-investigation information between organisations and across borders using CASE**, presented by Mattia Epifani and Nikolaos Matskanis.

Our presentation demonstrated the benefits of using the Cyber-investigation Analysis Standard Expression (CASE), an evolving, community-developed standard, which is intended to serve the needs of the broadest possible range of cyber-investigation domains. It explained the collaboration workflows between organisations and across country boundaries for the exchange of

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

electronic evidence, as well as the tools and services that have been developed and deployed by the EVIDENCE2e-CODEX Project in support of these workflows.

In addition, the secure infrastructure deployed by e-CODEX (e-Justice Communication via Online Data Exchange) was also explained, as EVIDENCE2e-CODEX is currently using the e-CODEX transfer services for the information exchange between criminal justice entities in Europe.

You can read more about the event here and here.

- **INSPECTr Kick-off Meeting**, 18-20 September 2019, Dublin, Ireland

The 'Intelligence Network & Secure Platform for Evidence Correlation and Transfer' (INSPECTr) Project is to develop a shared intelligent platform and a novel process for gathering, analysing, prioritizing and presenting key data to help in the prediction, detection and management of crime in support of multiple agencies at local, national and international level. This data will originate from the outputs of free and commercial digital forensic tools complemented by online resource gathering.

Using both structured and unstructured data as input, the developed platform will facilitate the ingestion and homogenization of this data with increased levels of automation, allowing for interoperability between outputs from multiple data formats. Various knowledge discovery techniques will allow the investigator to visualize and bookmark important evidential material and export it to an investigative report. In addition to providing basic and advanced (cognitive) cross-correlation analysis with existing case data, this technique will aim to improve knowledge discovery across exhibit analysis within a case, between separate cases and ultimately, between interjurisdictional investigations.

INSPECTr's Work Package 2 is dedicated to the development of a Reference Framework for Standardization of Evidence Representation and Exchange (SERE), building upon the results of EVIDENCE and EVIDENCE2e-CODEX projects and the further development of the CASE language (to be used for SERE) and its application in the Reference Implementation Portal by the EC. Providing a Reference Framework for SERE aims at:

- orchestrating 'standard' solutions for forensic investigations across EU LEAs;
- parsing of outputs of forensics tools to conform to standards;

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

- specifying provenance requirements for a CASE management system;
- defining an Information Exchange Policy to formalize obligations and controls for information;
- sharing and standardizing data protection markings.

A presentation on the achievements of the EVIDENCE and EVIDENCE2e-CODEX projects to serve as a basis for the future work on INSPECTr was made during the project kick-off meeting, 18-20 September 2019, in Dublin, Ireland. It served to familiarize the project partners with the main results and to deliver a true-to-life example of a use-case at hand.

EVIDENCE2e-CODEX EESP Application First Hands-on Exercise

EVIDENCE2e-CODEX, together with "Electronic Xchange of e-Evidences with e-CODEX" (EXEC) and the e-Evidence Project led by the European Commission, organized a two-day event engaging 66 technical and legal experts from the digital justice community to discuss and test the three projects' applications. The joint **Merging Views Workshop** took place in Florence, Italy, on 25-26 September 2019.

The event was focused on the achievements of the three projects.

- The **Evidence Exchange Standard Package (EESP) Application**, provided by EVIDENCE2e-CODEX, integrates the formal language for representing and supporting the electronic evidence exchange process (CASE) in an electronic evidence platform.
- The **e-Evidence Digital Exchange System**, provided by the EC, is the system that manages the EIO/MLA procedures/instruments: e-Forms, business logic, statistics, log, etc. The Reference Implementation is the front-end portal of the e-Evidence Digital Exchange System and is also provided by the EC.
- Both instruments are using **e-CODEX**, being the content agnostic e-Delivery infrastructure that supports cross-border e-Justice services. The

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

EXEC project is extending/strengthening some components of e-CODEX to manage the evidence exchange service.

The European experts reflected on several important aspects:

- Actions and progress on the legal issues for EIO and MLA in MSs;
- Practical labs for the use of the Reference Implementation Portal and the Evidence Exchange Standard Package Application;
- Interactions between the Evidence Exchange Standard Package Application and the Reference Implementation Portal.

Each session was organized around a technical overview and/or demo of the specific features, followed by a dedicated discussion.

All **presentations** given during the Workshop, including agenda, venue information, photos, etc. can be found on the EVIDENCE2e-CODEX website.

A total of 17 Member States (Austria, Bulgaria, Belgium, the Czech Republic, Croatia, Denmark, Estonia, France, Germany, Greece, Italy, Latvia, Luxembourg, Romania, Spain, and the Netherlands), alongside representatives of EUROJUST and EJN, took part in the **hands-on exercises** providing feedback and recommendations for improvement of the tools.

Evidence Exchange Standard Package (EESP) Application

We provided an overview of the technical activities undertaken within the EVIDENCE2e-CODEX Project to facilitate the understanding of the follow-up demonstration. Previous discussions focused on enabling the digital exchange of EIO and MLA legal instruments which would be a significant advance in the field of judicial cooperation. However, another essential element represents the evidence package itself, containing all the data and metadata. Returning to the transfer of an EIO request through the Reference Implementation Portal over e-CODEX, the evidence package could be exchanged as a simple attachment without any specific representation. Nevertheless, the use of a standard, in this case the USO/CASE language[1], offers numerous benefits:

- fostering interoperability,
- strengthening admissibility and trustworthiness, and
- enabling more advanced correlation and analysis, etc.

[1] The EESP application supports the Unified Cyber Ontology (UCO)/Cyber-investigation Analysis Standard Expression (CASE) language.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

This is the role and advantage offered by the EESP Application developed within the EVIDENCE2e-CODEX Project. The EESP relies on a web application that supports UCO/CASE language, the standard chosen for the representation of evidence package metadata. The EESP web application is used for the management and packaging of cyber-investigation information. It facilitates the transfer of the evidence package over the e-Evidence Digital Exchange System to the requesting competent authority. This is performed in accordance with the chain of custody and chain of evidence requirements while guaranteeing the confidentiality, authenticity, and integrity of data.

The potential uses of the EESP application include:

- creation of an evidence package following search and seizure;
- importing a report from a forensic tool into an evidence package, following forensic acquisition;
- reading the content of an evidence package;
- importing an evidence package from the competent authority of an executing state into the evidence package already in the hands of the competent authority of an issuing state;
- preparing an evidence package, including final report, for the competent authority of an issuing state.

EESP Application Interaction with the e-Evidence Digital Exchange System

The e-Evidence Digital Exchange System provides the secure platform required to execute an exchange over e-CODEX to the competent authority of another country. At national level it operates the Reference Implementation Portal which ensures interoperability with existing national systems, as member states are free to adopt their own national solution provided it fulfils the common requirements. The evidence package produced by the EESP application contains the secure data and metadata as collected. An important player in this process are the forensic laboratories and/or law enforcement experts that have the required competencies to deal with the varieties of evidence encountered as part of an investigation. In the context of this infrastructure's interaction with the EESP application, as can be seen from the figure below, an important aspect is ensuring that this multi-layered system remains user-friendly to encourage its voluntary endorsement by end-users.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

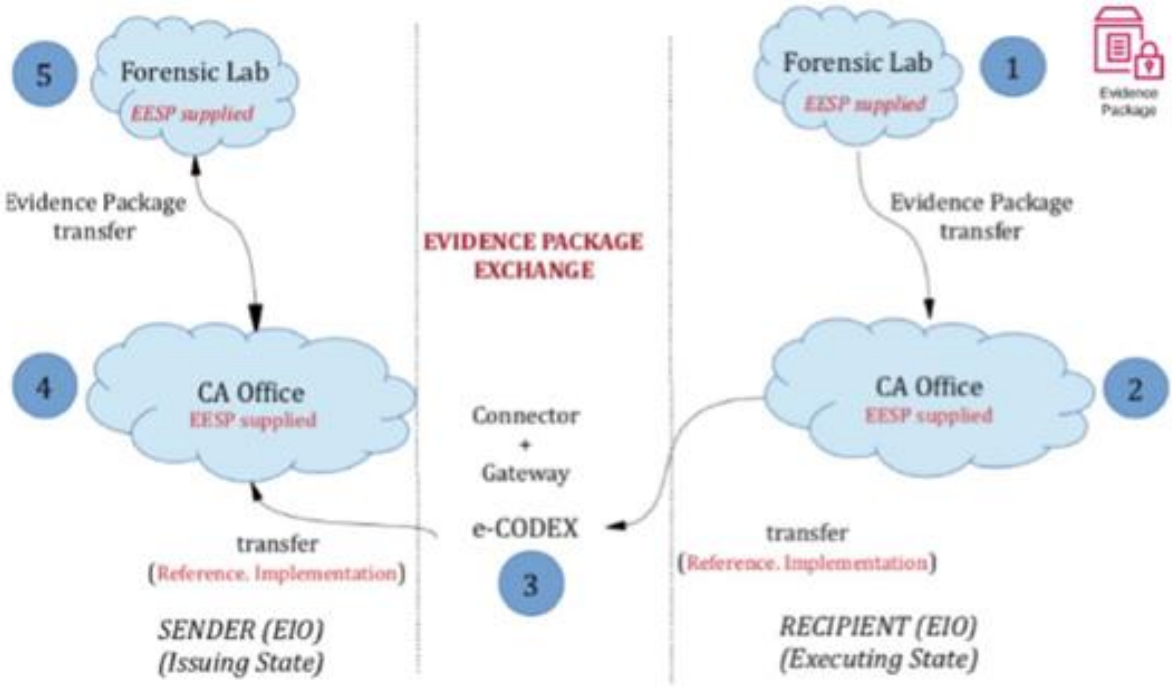


Figure 1: Evidence Exchange Scenario – Overview

EESP Application Use Case

In order to illustrate the EESP application's potential role in a real investigative case, the audience was presented with the investigation of a child grooming case via social media of a teenage girl living in Berlin:

> *The German competent authority authorized the acquisition of the girl's phone once the parents voluntarily handed it over to the LEA. The forensic acquisition was assigned to a German forensic laboratory, which used a specific forensic tool to perform the acquisition. An evidence package was created using the EESP application and was transferred to the German competent authority. The German competent authority received the evidence package and read its content. The extracted data revealed the involvement of an Italian man. As a result, the German competent authority issued an EIO through the Reference Implementation, to the Italian competent authority, requesting a search and seizure of the devices of the suspect and extraction of evidence from the seized items.*
>
> *The Italian competent authority authorized the search and seizure and assigned an Italian forensics laboratory to carry out the action, including the extraction of data from the seized devices. The Italian forensic*

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

laboratory carried out the search and seizure, created a forensic image of the hard disk of the seized computer and carried out a forensic extraction of the data, revealing images of the victim.

An evidence package was created with the EESP application and was transferred to the Italian competent authority. The Italian competent authority received the evidence package, read its content and sent back the evidence package including the images found on the hard disk to the German competent authority.

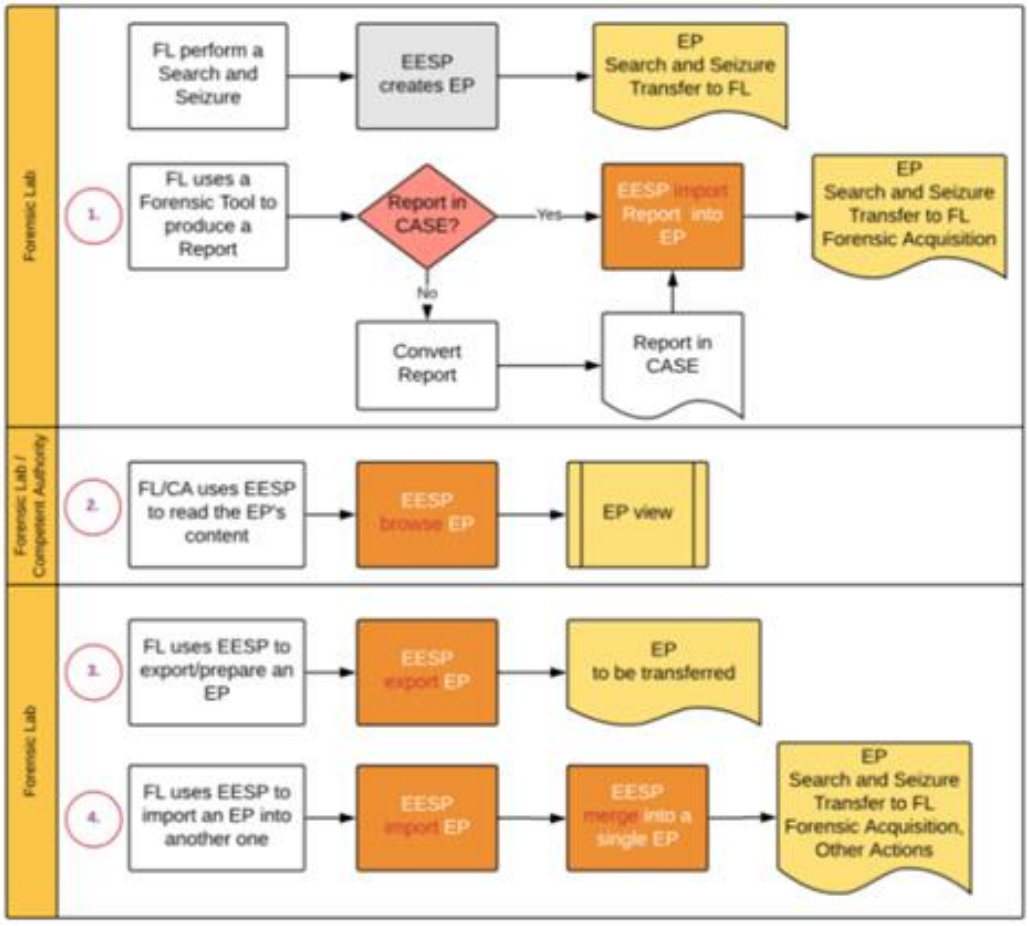


Figure 2: EESP uses in the communication between forensic labs/law enforcement and competent authority

Demonstration & Practical Sessions

The audience was presented with an overview of supporting tools developed for forensic laboratories and reminded about the existence of the Digital Forensics Tools Catalogue, an output of the EVIDENCE Project mapping over 1500 acquisition and analysis tools. Support was expressed for a general adherence to the CASE language in the development of future forensics tools, which would lessen the need

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

to rely on UCO/CASE Convertor tool. Given the rapid pace of digitalization, the technical aspects under discussion represent issues of increasing concern and relevance for practitioners. A range of matters were raised for consideration. The participants were unanimous about the need for competent authorities from the issuing state to be able to verify the content of an evidence package upon receipt from the forensics laboratory before sending it onwards to the competent authorities of the requesting state.

Numerous reasons were cited to this end, such as ensuring compliance with fundamental rights, verifying that the content does not affect national interests or checking that the request is fulfilled. This may be problematic as an oversight role requiring technical competences given the complexity of the forensic analysis process. In order to provide a comprehensive reply, the judicial authorities from cooperating states should communicate effectively and clearly define what is requested in order to avoid collecting and sharing disproportionate amounts of data which may be stored on a given device. Another issue touched upon concerns the relevance of the best evidence rule in the context of digital evidence, different to physical evidence from many perspectives and facing specific issues. Performing data extraction according to the best method available may amount to evidence tampering as the modifications may result in data loss otherwise accessible with a more recent tool or technical process. Given the constant progress in the field of forensics, it would me more appropriate to qualify electronic evidence as best available at a given point in time.

Furthermore, the use of standards for evidence management purposes, reinforces its validation in terms of comparison. The participants confirmed that so far, the exchange of digital evidence is mostly human based. However, the technical aspect of electronic transfer is increasingly gaining prominence, not only transnationally but also domestically when a forensic image needs to be transferred from one city to another. The acceptable security level for the transfer is a key matter and it is crucial to agree upon an acceptable minimum level between the Ministries of Justice involved in the implementation of digital transfer. This entails a trade-off between the level of security sought and the setup of cumbersome procedures to ensure it. Finally, the competent authorities are ultimately responsible for assessing the sensitivity of exchanged data in order to determine the appropriateness of relying on a particular means of transmission, including digital.

The rest of the meeting was dedicated to practical laboratories for the use of the e-Evidence Reference Implementation Portal. To this end the participants were divided by country intro groups of three and provided with a computer station. They could connect as the competent authority of the attributed country in order

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

to prepare an EIO request (i.e. fill in the required fields, experiment with the proposed functionalities by selecting specific boxes and filters) and connect afterwards as the competent authority of the executing state to review and reply to the EIO request. During the try-out sessions, the practitioners shared many comments and suggestions concerning different aspects of the Reference Implementation Portal (i.e. workflow structure, user interface, order of countries listed in the court database, date format, language acceptability) and made recommendations for improving the tool's functioning. The European Commission has been collecting feedback on requirements, changes and improvements through the regular expert group meetings it has been organizing with legal and technical representatives from the EU member states. This workshop provided an additional opportunity for gathering structured feedback by presenting practitioners with a preliminary version prior to the official launch. Interaction with the audience was also enabled via the Slido online platform where participants could share directly their input and thoughts of the tool.

Following the demonstrations and testing exercise, the audience engaged in an active discussion, widening the debate to other topics for consideration, including the platform's capacity, interoperability issues and its eventual accessibility for lawyers. Countries hold different approaches with regards to digital forensics examinations. Some only trust their public administration services, others which struggle with accumulated backlogs and delays authorize the hiring of external consultants to perform the forensic acquisition and examination. Hence some countries need to ensure their law enforcement authorities maintain up-to-date competencies and tools in the highly specialized area of digital forensics. Ultimately it is up to national authorities to decide whether they subcontract these services, or they commit to investing into expensive commercial tools and resources such as staff training.

Conclusions

The joint **Merging Views Workshop** workshop represents the culmination of EVIDENCE2e-CODEX efforts on stakeholder engagement with the project activities and results. It provided the opportunity to update representatives of the technical and legal communities on the status of the EVIDENCE2e-CODEX project alongside that of EXEC and e-Evidence Projects. Furthermore, it allowed for a detailed demonstration of the EESP Application and actual testing of the Reference Implementation Portal. The meeting enabled the project team to gather valuable feedback from technical experts and prospective end-users on the tools' functioning following their cross-fertilization within the context of practical sessions. It also benefitted from the expertise of national experts involved in the

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

e-Evidence working groups. This enabled a comprehensive and multidisciplinary appraisal of the EESP Application by combining complementary perspectives and debating diverging positions. This will contribute to the tools' fine-tuning as the project approaches its completion and in preparation of the final conference that will be jointly held on 21-22 January 2020.

EVIDENCE2e-CODEX Final Project Event

To the project end we are organizing one more public event, namely the EVIDENCE2e-CODEX Final Conference, 21-22 January 2020, Brussels, Belgium. It will be jointly organized between EVIDENCE2e-CODEX, "Electronic Xchange of e-Evidences with e-CODEX" (EXEC) and the e-Evidence project led by the European Commission.

Save the date and stay tuned on the details!

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468