

Deloitte.



Cyber Forensic Services

Deloitte | Hungary

Why Deloitte?

Deloitte is one of the world's largest consulting firm, employing more than 300,000 professionals globally



\$47.6B

Revenues (2020)



334,000

Employees (2020)



700+

Office



150+

Country



88,820

New Colleague (2020)



\$265M

Total societal investments (2020)

Services

Our seven global service profiles:

- Audit & Assurance
- Consulting
- Risk Advisory
- Financial Advisory
- Legal
- Tax
- Deloitte Private



Global presence

- North and South America:
 - 244 offices
 - 149,760 staff
- EMEA:
 - 522 offices
 - 109,340 staff
- Asia:
 - 103 offices
 - 75,730 staff



Industries and sectors

- Technology, Media & Telecommunications
- Financial institutions sector
- Government & Public Services
- Service centres
- Energy, Resources & Industrials
- Life Sciences & Health Care
- Manufacturing sector



Regional presence in Central Europe

- 44 offices
- 18 countries
- 6,900+ experts
- We are the region's largest and longest established professional services firm



Why Deloitte?

Deloitte Global Cybersecurity Services (CRS)

“Our services go beyond technical vulnerability assessments. We translate technical issues found to business risks.”



More than 500 vulnerability assessments per year



Diverse selection of clients including financial services, telecom, manufacturing and automotive



Centre of Excellence for Cyber Security Services in Central Europe



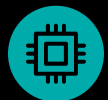
Collaborative approach with Deloitte member firms throughout the world



Highly skilled specialists in the area of e-discovery, forensic services and malware analysis



Specialized professional team for security testing and training



Unique hardware analysis services



Why Deloitte?

Deloitte Hungary's Cyber Forensic Services

Deloitte Cyber Forensic team in Hungary has **twenty years of experience** in investigations and computer forensics.



Deloitte's **global network** allows us to conduct extensive fact-finding investigations anywhere in the world, to deliver broader solutions to clients from proactive consulting and investigations to remediation.



**DELOITTE
CYBER
FORENSIC
TEAM**

We **helped** many clients to **detect and respond to the risks** that come from various types of fraud, corruption, bribes, financial mismanagement and other misconduct.



We combine our highly **specialized skills** in the areas of corporate investigations, cyber security, FCPA, and anti-fraud consulting with deep financial acumen and advanced analytics.



Deloitte Hungary | Cyber Forensic Services

When might you need us?

Malware Attacks

A malware attack is when cybercriminals create malicious software that's installed on someone else's device without their knowledge to gain access to personal information or to damage the device, usually for financial gain. Different types of malware include viruses, spyware, ransomware, and Trojan horses.

Phishing / Vishing / Smishing Attacks

Phishing / Vishing / Smishing attacks involve attackers posing as a credible source to obtain sensitive information, usually usernames, passwords, credit and debit card details.

Business E-mail Compromise Attacks

These attacks involve the perpetrators posing as a trusted source to send e-mails to the victims. This is designed to obtain critical business and financial information, thus misleading employees of the attacked company to transfer large sums of money to the perpetrators' bank account.

Ransomware

Ransomware attacks deny the victim's organization the ability to operate their IT systems and access their critical data until a ransom is paid to the attacker.



Insider Threat

A malicious insider, either an employee or contractor, can use their legitimate access to an organization's IT environment to steal data for personal gain or to cause damage to the organization. This occurs through disrupting normal operations or publicly leaking data to reduce trust in the organization.

Identity Theft

In the case of identity theft, the attacker obtains the victim's personal information and uses it to commit fraud.

Advanced Persistent Threat

A targeted attack from an advanced adversary can lead to the loss of intellectual property and sensitive user data as well as potential sabotage and damage to the IT infrastructure.

Data Leakages

Data leaks involve unauthorized persons obtaining personal, sensitive or confidential data. Documents affected by a data leak are disclosed and/or shared without permission.

Social Engineering

Social engineering is the art and science of getting people to comply with our wishes. A social engineering attack uses psychological manipulation and other techniques and procedures to get sensitive information or access to certain systems.

Deloitte Hungary | Cyber Forensic Services

When might you need us?

Offences Against Property

Crimes against property are the oldest and longest sanctioned crimes. The legal object of these crimes is usually property rights, so in such criminal cases, the offender does not commit a crime against the victim but acquires or damages the victim's property or assets. These offences include fraud, economic fraud, information system fraud, embezzlement, misappropriation of funds, defalcation.

Crime Against Consumer Rights and Any Violation of Competition Laws

By penalizing these acts, the legislators aimed to protect the interests of consumers and the fairness of economic competition. The legal object of the offences is the freedom and fairness of competition, the unrestricted operation of the free market and the interest in the transparent and fair use of public funds and budgets. The category includes the following punishable acts: breach of business secrecy, imitations of competitors, agreement in restraint of competition in public procurement and concession procedures.

Illicit Access to Data and Crimes Against Information Systems

These offences cover certain types of conducts involving information systems. By sanctioning these offences, the legislator intends to protect the public interest for the proper functioning of information systems and for the preservation of the data contained in them. These offences include the following: illicit access to data, breach of information system or data, compromising or defrauding the integrity of the information system protection solution or device.

Economic and Business-Related Offences

Economic crime should be understood as a form of criminal activity during the management of business processes. In addition to possible damage to individual interests, it is capable of damaging or endangering primarily and typically the order and obligations of management, and the framework of fair and lawful management. Economic crime includes offences against the proper conduct of business, such as breach of accounting regulations, fraudulent bankruptcy, impairment of own capital, unauthorized financial activities and insider dealing.

Other Criminal Offences When You Might Need Us

Defamation, slander, extortion and other legal offences that may harm the economic interests of our clients.

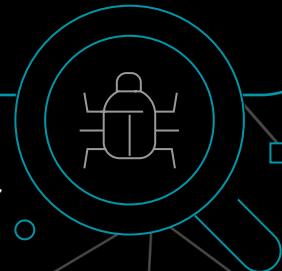


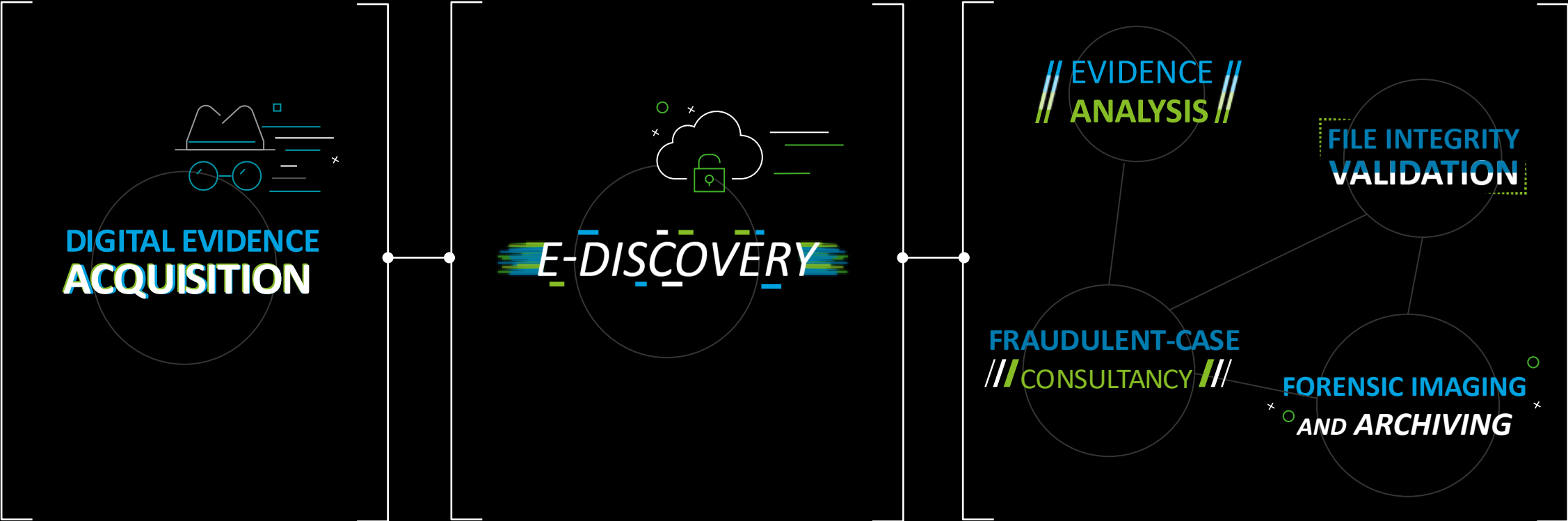


Our Solutions

Many years of experience allow us to facilitate a cohesive and effective atmosphere, where preference is in effective **communication and questioning**. Our Cyber Forensic team is supported by our highly secured **Forensic Lab**, to benefit clients in all aspects of forensic scenarios, including prevention, detection and investigation in the following **interdisciplinary areas**.

FORENSIC INVESTIGATION







*For many organizations, a **cyber incident** is not a question of "if", but "when".*

*Deloitte Hungary Cyber Forensic Services is a **comprehensive service line** which guides and supports our clients in combatting **internal and external fraud exposure**.*



Deloitte Hungary | Cyber Forensic Services

Computer Forensics

Deloitte supports clients in **all aspects of computer forensics** by focusing on the value of evidences. Chain of custody is kept at all stages of the discovery process and the integrity of the evidences stands beyond doubt.






We use **dedicated software** to analyze and search digital evidences to ensure we uncover the key pieces, which we review manually to ensure their relevance in terms of the case.

Services include:

-  Digital evidence acquisition
-  Forensic imaging and archiving
-  Evidence analysis
-  E-Discovery
-  File integrity validation

What we excel in:

-  Twenty years of forensic experience
-  Highly skilled and experienced Cyber professionals
-  Our Cyber Forensic Team is supported by our highly secured Forensic Lab

*It takes a complex journey
to unravel the truth:
one must ask the **right question**
to get the **truthful answer.***

*That is why our interviewing
methods are **based on science.***



Deloitte Hungary | Cyber Forensic Services

Investigating Fraudulent Cases

Deloitte has strong skills to help clients **act quickly and confidently** against regulatory concerns, actions and/or sensitive internal investigations of fraud, corruption and misconduct.



Our **regional and global network** allows us to combine an understanding of local business cultures and regulatory issues, to find a path towards a successful resolution and leave the client better prepared to protect their assets and reputation.






We believe in the power of **personal connections** and **adequate communicational style** which serve as the basis for successful interviewing, when investigating fraudulent cases for clients.

Interviewing or "thematic conversation with people" is an essential part of every investigation. We gather information with **empathy and discretion**, whether it is from victims, witnesses or accused parties.

Services include:

-  Document review and collection
-  Interviewing and Interview Training
-  Investigation of fraudulent cases
-  BIS (Business Intelligence Services)
-  Special expert involvement
-  Fact finding report
-  Deloitte Halo, our end-to-end whistleblowing service

What we excel in:

-  Twenty years of forensic experience
-  Conscious and precise planning
-  Integrating the methods of cognitive science and forensic interviewing techniques

Deloitte Hungary | Cyber Forensic Services











Advanced Interview Training

Our two-day training gives you the opportunity to learn the key principles of **non-confrontational interviewing**. Audience will learn how to assess verbal and non-verbal behavior and become more effective on the focus of an investigation for obtaining reliable information, while containing situations. This training course offers a broad range of cutting-edge methods to conduct more effective interviews, resulting in identifying the truth more efficiently and with less resistance.



This course applies specifically to organizations whose personnel may be called upon to interview individuals and investigate incidents and cases at a first phase. **Internal auditors, law enforcement professionals, HR personnel, security and compliance, government personnel** and anyone conducting these inquiries will learn how to apply the interview techniques which aim to uncover the truth and bring these cases to a successful conclusion.

Services include:

-  Reasons for interviewing
-  Sequence of interviews
-  Interview protocol
-  Planning the interview
-  Environment of the interview
-  Victim, witness and suspect interview
-  Cognitive science like memory
-  False admission and other dishonesty
-  Lie detection
-  Documenting the interview

Deloitte Hungary | Cyber Forensic Services

The Team | Leaders

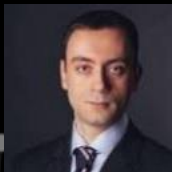
The Cyber Forensic team in Hungary has 40+ Cyber professionals, most of whom are trained for and experienced in capturing digital evidences, handling incidents, secure leaving and forensic investigations and trainings.



Lajos Antal is the Cyber Risk Services Leader of Deloitte Central Europe and leads Forensic engagements in Hungary. Lajos has over 20 years of experience in the field of Cyber Risks and Forensics. He has been a Deloitte Partner for over 10 years. Beside dealing with economic crimes, mostly bribery and various types of frauds and misconducts, he is highly experienced in interviewing.



Csilla Szalai has been with the Cyber Forensic team of Deloitte Central Europe since 2009. Having a main focus on managing major projects and liaising with Project Managers and leadership she has a comprehensive overview of the Cyber projects including Forensic engagements in Hungary. She is also actively dedicated to executing proper Forensic management solutions. Csilla is also qualified as a private investigator, which helps her to successfully investigate cases of suspected fraud and abuse.



István Herédi is a manager in the Digital Forensics team. He has been focused in the past four years on meeting challenging client expectations, on both the managerial and technical level. István has extensive skills in forensic e-discovery and password cracking scenarios and holds the Certified Hacking Forensic Investigator certification.



Klára Mokdad is working as a manager in the Deloitte Cyber Risk Services team. Klára focuses on forensic investigative interviewing, organizational fraud, forensic projects, and facilitates the Advanced Interview Training. Previously, she worked for International Organizations, the EU and Non-profit organizations. She has many years of experience in sectors and organizations which enhanced her analytical, communication and cross-cultural skills.

Deloitte Hungary | Cyber Forensic Services

The Team



Sandor Hentes is a Specialist Manager in the Cyber Risk Services group of Deloitte Hungary's Risk Advisory department. He has more than 13 years experience in the IT Security industry, main profile is penetration testing, network-, application-, and physical security, social engineering and network forensic. Experienced in network planning, project management, and has more than six years hands-on experience in incident handling, Unix/Linux system and large scale network administration, software development.



Barbara Bodrogi is a senior consultant in the Deloitte Cyber Risk Services team. Barbara works on complex forensic engagements and is a co-trainer in the Advanced Interview Training. She graduated in Psychology from the University of Pécs. Having previous experience in clinical and cognitive psychology, her ambition is to help clients understand the mechanisms of human thinking and behavior relating to deception and interview situations. Barbara received her training as a social skills trainer at the Budapest University of Technology and Economics. She is currently pursuing her doctoral studies at the University of Pécs in Evolutionary and Cognitive Doctoral Programme.



Evelyn Littvan is a consultant in the Cybersecurity Services team of Deloitte's Risk Advisory department. She earned her juris doctor degree at Pázmány Péter Catholic University. She is currently studying cybersecurity at Óbuda University. Evelyn has prominent experience in investigating white-collar and Cyber crimes at The Hungarian National Bureau of Investigation's Cyber Crime Department, and The National Institute of Criminology where she previously held her internship. She is highly experienced in interrogation. Evelyn focuses on forensic investigative interviewing, forensic projects, and is facilitating the Advanced Interview Training.

WE MUST TAKE ACTIONS

TO ENSURE
SECURITY





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see deloitte.hu/about to learn more.

In Hungary, the services are provided by Deloitte Auditing and Consulting Limited (Deloitte Ltd.), Deloitte Advisory and Management Consulting Private Limited Company (Deloitte Co. Ltd.) and Deloitte CRS Limited (Deloitte CRS Ltd.), (jointly referred to as “Deloitte Hungary”) which are affiliates of Deloitte Central Europe Holdings Limited. Deloitte Hungary is one of the leading professional services organizations in the country providing services in four professional areas - audit, tax, risk and advisory services - through more than 750 national and specialized expatriate professionals. Legal services to clients are provided by cooperating law firm Deloitte Legal Göndöcz and Partners Law Firm.

These materials and the information contained herein are provided by Deloitte Hungary and are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s).

Accordingly, the information in these materials is not intended to constitute accounting, tax, legal, investment, consulting, or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

These materials and the information contained therein are provided as is, and Deloitte Hungary makes no express or implied representations or warranties regarding these materials or the information contained therein. Without limiting the foregoing, Deloitte Hungary does not warrant that the materials or information contained therein will be error-free or will meet any particular criteria of performance or quality. Deloitte Hungary expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy.

Your use of these materials and information contained therein is at your own risk, and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte Hungary will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained therein.

Differently from the above written, in case the information and materials are expressly provided as final performance of a contract concluded between you and Deloitte Hungary, Deloitte Hungary takes liability that the service has been provided and the product - if any - has been prepared contractually. Deloitte Hungary declares that the materials and information serve the persons / entities assigned and are suitable for the purposes determined in the contract. Deloitte Hungary excludes all liability for damages arising out of or in connection with the documents, materials, information and data provided by you. For all the questions not ruled herein, the relating contract shall be applicable.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.