Ali Dehghantanha, PhD

Founder and Principal, Inference Forensics

Toronto, Ontario, Canada | ali@inferenceforensics.com | inferenceforensics.com

Current as of 22 November 2026

Profile

Ali Dehghantanha is the Founder and Principal of Inference Forensics, an AI forensics firm in Toronto, Canada, and leads each of its engagements. His work is AI forensics: establishing how and why an AI system reached a decision, or failed to. Before a dispute, he assesses whether an organization's AI systems keep enough evidence to reconstruct and defend an individual decision. After one, he establishes which model, version, instructions and data were in force during a specific interaction, what the system actually did, and whether the surviving records are sufficient to support a finding. His AI forensics work builds on fifteen years of teaching and research in digital forensics, beginning with undergraduate digital forensics courses in 2011, and includes peer-reviewed forensic case studies in the Journal of Forensic Sciences and Science & Justice.

Positions

Years	Role	Institution
2026 to present	Founder and Principal	Inference Forensics, Toronto, Canada
2024 to present	Full Professor, School of Computer Science	University of Guelph, Canada
2020 to present	Tier 2 Canada Research Chair in Cybersecurity and Threat Intelligence	University of Guelph, Canada
Current	Director, Canada Cyber Foundry; Director, Cyber Science Lab	University of Guelph, Canada
2026	Fulbright Canada Visiting Scholar (Fulbright Canada Scholar Entrepreneurship Award)	University of California, Berkeley, USA
2020 to 2024	Associate Professor, School of Computer Science	University of Guelph, Canada
2018 to 2020	Assistant Professor, School of Computer Science	University of Guelph, Canada
2017 to 2018	Senior Lecturer / Associate Professor	University of Sheffield, UK
2015 to 2017	Marie Curie International Incoming Fellow	University of Salford, UK
2011 to 2015	Senior Lecturer, Information Security Group	Universiti Putra Malaysia

He was also Adjunct Associate Professor, Department of Electrical and Software Engineering, University of Calgary (2020 to 2024). At Guelph he established the Master of Cybersecurity and Threat Intelligence (2019) and a second graduate cybersecurity program (2024), and leads the NSERC (Natural Sciences and

Engineering Research Council of Canada) CREATE SECURE-AGRO training program. He has taught digital forensics at undergraduate and graduate level in Malaysia and the UK.

Areas of expertise

- **AI forensics:** reconstruction of AI and agentic system behaviour in a historical interaction; attribution of outputs and actions to a model build, configuration and context; log-based attribution in multi-agent large language model (LLM) systems; assessment of whether retained logs and artifacts can support a finding.
- **Evidence preservation and forensic readiness:** what an organization must capture, and how, for AI-assisted decisions to be examined later by a court, regulator or insurer.
- **Digital forensics:** cloud, mobile, gaming and Internet of Things (IoT) investigations, anti-forensics, and forensic examination of synthetic (deepfake) media.
- **Malware analysis and cyber threat attribution:** machine-learning-based malware detection, threat hunting and attribution of attacks to actors and campaigns.

Expert evidence and public testimony

- Invited expert witness, House of Commons Standing Committee on Industry and Technology (INDU), study on artificial intelligence in Canada's strategic industries, Ottawa, 23 March 2026.
- Public submission to Innovation, Science and Economic Development Canada (ISED), AI transparency consultation, "Two Kinds of Transparency", on forensic-readiness conditions for federal AI procurement, September 2026.
- Written evidence to the UK Information Commissioner's Office (ICO), Call for Evidence on Agentic AI, on behalf of Cyber Science Lab, on the minimum tamper-evident record needed to reconstruct consequential AI agent actions and automated decisions under UK GDPR, October 2026.
- Expert commentary, CBC News (I-Unit), on the Crime Stoppers / Navigate360 tip-line data breach, including an on-camera interview, October 2026.
- Expert commentary, Global News, on the string of major technology outages, November 2026.
- Commissioned technical report, Royal Military College of Canada and Department of National Defence (2022): detection, attribution and forensic examination of deepfake image, video and audio.
- Member, The Sedona Conference Working Group 7 (Sedona Canada), on principles for electronic discovery and digital evidence (2026 to present).
- Member, UNESCO AI Ethics Experts Without Borders, Global AI Ethics Observatory (2026 to present).

Selected invited talks to forensic, legal and law-enforcement audiences

- "Forensic Analysis of Machine Learning Agents", Summer School on Computational Forensics, Oslo, Norway, August 2019.
- "Enhancing Collaboration between Academia and Law Enforcement Agencies in Digital Forensics", Canadian Association of Chiefs of Police, ICT Committee Blue Team Summit, Vancouver, February 2020.
- "Forensic Readiness: Is Your Company Ready for a Forensics Examination", ISACA Cyber Security Nexus, London, UK, November 2016.
- "Malware Trends and Lessons for Law Enforcement Agents", European Intellectual Property Prosecutors Network workshop, Alicante, Spain, March 2016.

Selected publications

AI forensics and AI systems

1. Dehghantanha, A., and Homayoun, S. AI Forensics Across White-, Grey-, and Black-Box Access: A Process Model and Research Agenda for Post-Incident Investigation of AI Systems. arXiv:2608.03520, 2026.
2. Rabieinejad, E., Zarrinkalam, F., and Dehghantanha, A. Beyond the prompt: Log-based threat detection and attribution for multi-agent LLMs. *Information Processing & Management*, 2026. doi:10.1016/j.ipm.2026.104768
3. Dehghantanha, A., and Homayoun, S. SoK: The Attack Surface of Agentic AI: Tools and Autonomy. arXiv:2603.22928, 2026.
4. Yazdinejad, A., Dehghantanha, A., Karimipour, H., Srivastava, G., and Parizi, R. M. A robust privacy-preserving federated learning model against model poisoning attacks. *IEEE Transactions on Information Forensics and Security*, 2024. doi:10.1109/TIFS.2024.3420126
5. Nowroozi, E., Dehghantanha, A., Parizi, R. M., and Choo, K.-K. R. A survey of machine learning techniques in adversarial image forensics. *Computers & Security*, 2020. doi:10.1016/j.cose.2020.102092

Digital forensics

6. Teing, Y.-Y., Dehghantanha, A., Choo, K.-K. R., Conti, M., and Dargahi, T. Forensic investigation of cooperative storage cloud service: Symform as a case study. *Journal of Forensic Sciences*, 2016. doi:10.1111/1556-4029.13271
7. Taylor, P. J., Mwiki, H., Dehghantanha, A., Akinbi, A., Choo, K.-K. R., Hammoudeh, M., and Parizi, R. Forensic investigation of cross-platform massively multiplayer online games: Minecraft as a case study. *Science & Justice*, 2019. doi:10.1016/j.scijus.2019.01.005
8. Conti, M., Dehghantanha, A., Franke, K., and Watson, S. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 2017. doi:10.1016/j.future.2017.07.060
9. Teing, Y.-Y., Dehghantanha, A., and Choo, K.-K. R. Forensic investigation of P2P cloud storage services: BitTorrent Sync as a case study. *Computers & Electrical Engineering*, 2016. doi:10.1016/j.compeleceng.2016.08.020
10. Daryabar, F., Dehghantanha, A., and Choo, K.-K. R. Cloud storage forensics: MEGA as a case study. *Australian Journal of Forensic Sciences*, 2016. doi:10.1080/00450618.2016.1153714

Malware and threat attribution

11. HaddadPajouh, H., Dehghantanha, A., Khayami, R., and Choo, K.-K. R. A deep recurrent neural network based approach for Internet of Things malware threat hunting. *Future Generation Computer Systems*, 2018. doi:10.1016/j.future.2018.03.007

Edited books

12. Choo, K.-K. R., and Dehghantanha, A. (eds.). *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Elsevier, 2016.
13. Choo, K.-K. R., and Dehghantanha, A. (eds.). *Handbook of Big Data Analytics and Forensics*. Springer, 2021.
14. Dehghantanha, A., Conti, M., and Dargahi, T. (eds.). *Cyber Threat Intelligence*. Springer, 2018.

Research record and credentials

- Among the ten most-cited researchers in digital forensics worldwide (Google Scholar); on the Stanford and Elsevier list of the top 2% of scientists every year since 2022. 92 journal and 24 conference papers; 6 edited books; 2 published US patent applications on adversarial attacks against machine learning systems.
- University of Guelph Research Excellence Award (2022); College of Engineering and Physical Sciences Research Excellence Award (2020), cited for excellence in cybersecurity and digital forensics.
- Fulbright Canada Scholar Entrepreneurship Award, Visiting Scholar at the University of California, Berkeley (2026); Marie Curie International Incoming Fellowship (2015).
- Certified Information Systems Security Professional (CISSP), since 2012; Certified Information Security Manager (CISM), since 2014. Senior Member, IEEE (2017) and ACM (2023).

Peer-reviewed forensics research grants (Principal Investigator)

Years	Funder and project
2019 to 2025	NSERC Discovery Grant, Artificial Intelligence-Aided Digital Forensics Examination
2020 to 2025	Canada Foundation for Innovation, John R. Evans Leaders Fund, Critical Infrastructure Protection: Forensics, Assurance, Analytics
2018 to 2019	Department of National Defence, Innovation for Defence Excellence and Security (IDEaS), Multiview Fuzzy Consensus Clustering for Cyber Threat Attribution
2015 to 2018	European Commission, Marie Curie International Incoming Fellowship, Privacy4Forensics: A Formal Rule-Processing Engine for Privacy-Respecting Forensic Investigation

Education

PhD, Security in Computing, Universiti Putra Malaysia, 2011. MSc, Security in Computing, Universiti Putra Malaysia, 2008. BASc, Software Engineering, Azad University of Mashhad, Iran, 2005.