AI is the use of machine or software intelligence instead of humans or animals some examples of AI being used are Alexa or Siri, ChatGPT, and self-driving cars[5]. Digital forensics is the branch of forensics science that involves identifying, acquiring, processing, analyzing, and reporting on data that is electronically [6]. The importance of studying both AI and digital forensics is because as we develop more advanced technology these two concepts are bound to intersect with each other. Eventually, we are going to want to have automated tools that will just output an answer for us or that find the information we need when we input certain items. This is where AI and digital forensics can interconnect with each other as we might want to use AI to accelerate the process of finding evidence or creating reports. Or the opposite of using digital forensics tools to figure out if someone has used AI incorrectly or unlawfully.

The history of how digital forensics came to happened in 2001 on August 7-8 when over 50 university researchers, computer forensics examiners, and analysts attended. At this meeting, they discussed how 4 topics in the new field of Digital Forensics Science these topics were: Define a Framework for Digital Forensic Science, Discuss the Trustworthiness of Digital Evidence, Discuss Detection and Recovery of Hidden Data, and Discuss Digital Forensic Science in Networked Environments (Network Forensics) [3]. These topics will be updated and changed over the next several years even up until today. The evolution of AI in digital forensics over the years has been relatively new. Using AI in digital forensics has been in identifying and investigating cybercrimes[2]. This has helped forensics specialist quickly identify and solve their problems. Some other methods that AI has helped in digital forensics are knowledge representation, expert systems, and pattern recognition as using AI in these has been very useful.

Some areas that AI has been used in have been tools such as chatGPT in which the user inputs a prompt of some kind and the AI spits an output based on what was prompted. Another area has been in image creation which works the same way as chatGPT in which the user inputs various suggestions and the AI ‘creates’ an image based on what it is given. And lastly, it can be used in the area of the analysis of plagiarism in reports and papers to determine if the user has plagiarized. Some of the advantages that AI can have are the elimination of human error and risk the difference between machines and humans is that humans naturally make mistakes even when they don’t want to because not everyone is created perfectly[1]. So using AI for repetitive tasks can eliminate that at a certain point humans are going to get tired and mess up unlike AI which can keep going on forever or until it shuts down. Another example of the use of AI without the risk or error of humans is sending AI machines into areas that humans couldn’t go to because of health risks. Another advantage is availability as AI is just a machine so it can be available 24/7 as humans can only be available for a certain number of hours a day. Because of this machines can work all day and AI programs or bots can answer questions immediately when people need it. Some disadvantages or limitations are changes in lack of creativity or emotion because of this AI is not useful for the artistic fields[1]. Another is when decisions are to be made that are sensitive AI is not equipped for this as AI can’t take emotions in the decision unlike humans can which may result in an AI making a decision that could result in negative ramifications. No improvement in experience is another disadvantage as AI can’t naturally learn from its own experience and mistakes. With humans they can do this naturally if an AI tries to do this it can be difficult and expensive. Although some programs have done this such as AlphaGo or the video called Hello Neighbor.

An AI tool currently used that was found is IBM Security QRadar Suite which is a modernized threat detection and response solution designed to unify the security analyst experience and accelerate their speed across the full incident lifecycle[7]. It uses enterprise-grade

AI and automation to increase analyst productivity and help resource-strained security teams work more effectively. One of the ways that AI is utilized is during its Unified analyst experience which uses its intuitive user interface to empower analysts to work more quickly and efficiently throughout their investigation and response processes, with shared insights and automated actions across products. By using unique, enterprise-grade AI capabilities, analysts can automatically contextualize and prioritize threats. In the suite, there is a product called the IBM Security QRadar EDR one of its features the behavioral tree uses an AI-friendly visual storyline that helps the analyst to speed up their investigation and response [9]. One limitation of this AI tool could be that it needs internet since it connects to a cloud service which also brings up the limitation of space or response time as a limitation. One of the benefits of the limitations is something that came up while searching the website in the features it states that in the federated search which allows you to search data in the cloud or on-premises in a single unified way which will free up IT resources. Another benefit is in delivered as SaaS on an AWA it allows you to get up and run quickly without needing for continuous updates or management which enables you to focus on the more important vulnerabilities and anomalous conditions. A case study with Sutherland Global Services added advanced threat detection and response capabilities of the IBM Security QRadar Suite to its existing security processes and toolset. They used the QRadar solutions to conduct real-time analysis of log data, network traffic, and security events and applied AI-based anomaly detects and more. In doing this Sutherland achieved several key results such as a faster mean time to detect security threats which was reduced from days or weeks to just hours, faster response time to minimize potential damage, and also cost savings due to reduced reliance on manual monitoring and interventions, and much more.

The ethical concerns with AI in digital forensics could be that because AI doesn't have the ability to have emotions certain decisions could be racially biased [11] this is explained in the study which resulted in the AI assigning more negative emotions to people that were other races other than white[10]. This could be bad in digital forensics as it can increase inequality in certain situations. Another concern is about privacy in data gathering and the sharing of data. Since data can be collected for a purpose and stored to be used for future purposes without the person's knowledge. Or using that data way after the person's been gone[11].

A prediction for the future of AI and digital forensics is that as technology gets more and more advanced and there is a push for AI it will eventually be used in digital forensics to help investigations. There will be a lot of legal concerns and questions that will delay the use of AI with digital forensics until there is a safe and proper way to use AI that is agreed upon in a positive scenario. In a negative scenario, there will be a huge push for AI in digital forensics and every other field that will identify tools that will help with the investigation in digital forensics but will output biased results and wrongful accusations because of people pushing for it to be used as a way to reduce cost. With the people using the tools realizing the results, there will be huge legal battles and laws put in place to allow the use of AI without the wrong results being identified. Some new applications that might be discovered and helpful will be an application that performs pattern recognition linguistically to help identify if a certain person or group is doing the crime since their previous crimes will be stored and will be able to be used. Another one might be network traffic analysis in which teams can train an AI algorithm to analyze network packets automatically, identify deviations from the normal traffic patterns, and issue alerts when an anomaly shows up to initiate an investigation. They can also assist in correlating network events with previous known attack patterns which will provide insight to the response team.

The research findings during this report have been that while AI has been used in many other ways such as security reasons there don’t seem to be many tools with AI that are used in digital forensics[12]. There are ideas of how AI can be used in digital forensics but nothing that is currently being used in official digital forensics besides company tools they’ve developed with AI features. Although AI is a fairly new concept it still has a lot of way to go in terms of ethical concerns and implementation on huge levels. The major concerns that are brought up about AI are the privacy of data such as repurposing, spillage, and persistence as well as transparency about how the AI will be used and what exactly for [11]. As well as the threat that AI will eventually replace all humans because of big corporations trying to cut money expenses.

References:

[1]“What are the advantages and disadvantages of artificial intelligence (AI)?,” *Tableau*. https://www.tableau.com/data-insights/ai/advantages-disadvantages#advantages

[2] L. Aggarwal. (2021 June). “The Evolving Roles and Applications of Artificial Intelligence in Digital Forensics”. *International Journal of All Research Education and Scientific Methods (IJARESM)* [Online]. vol 9, issue 6. Available: https://d1wqtxts1xzle7.cloudfront.net/67655150/FINAL_PUBLISHED_ARTIFICIAL_INTELLIGENCE_CYBER_SECURITY_RESEARCH_PAPER-libre.pdf?1623936048=&response-content-disposition=inline%3B+filename%3DThe_Evolving_Roles_and_Applications_of.pdf&Expires=1701581247&Signature=ateIn740-R~nbHjPg0Gq1vLyqghyVyLSl2et9-qyBgr10t0bqlnzyrmk5OgYYvKDJWEYmgvhYbuQAySbaQCLt1yC3YtF9qwkoAq717UJFT1ElaggfGzyDc8IQv1QzAIRcowpFrK8Rpf5YEPZtbKqqRsxjMAyrdgZZI2-WS0lO355tH98yKkDmhAfyB54V9nWWdunVpH5OMs927WEtxwt9YlpCL0q2fMkMYlYMWUy-0aHQVHdOLBBjvYHxPEkvF1kS9JJkK~2LIienLBvZaBu8WFEI1tVf8EfNg6bPZ~29vnYSPsr~V3dggdkT5ZIxMia-2tqPA4p1MRse5C~q9pIjg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[3] “A Road Map for Digital Forensic Research Collective work of all DFRWS attendees From the proceedings of.” Available: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

[4] “The Use of Artificial Intelligence in Digital Forensics: An Introduction,” *heinonline.org*. https://heinonline.org/HOL/P?h=hein.journals/digiteeslr7&i=35 (accessed Oct. 09, 2022).

[5]Wikipedia Contributors, “Artificial intelligence,” *Wikipedia*, Feb. 18, 2019. https://en.wikipedia.org/wiki/Artificial_intelligence

[6] Interpol, “Digital forensics,” *www.interpol.int*, 2023. https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch

[7] IBM, “IBM Security QRadar XDR,” *www.ibm.com*. https://www.ibm.com/qradar

[8] “Sutherland Global Services | IBM,” *www.ibm.com*. https://www.ibm.com/case-studies/sutherland

[9] “Security QRadar EDR | IBM,” *www.ibm.com*. https://www.ibm.com/products/qradar-edr

[10]L. Rhue, “Emotion-reading tech fails the racial bias test,” *The Conversation*, Jan. 03, 2019. https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404

[11] “The ethics of artificial intelligence (AI),” *Tableau*. https://www.tableau.com/data-insights/ai/ethics

[12]“6 Ways AI Can Revolutionize Digital Forensics,” *www.darkreading.com*. https://www.darkreading.com/application-security/6-ways-ai-can-revolutionize-digital-forensics