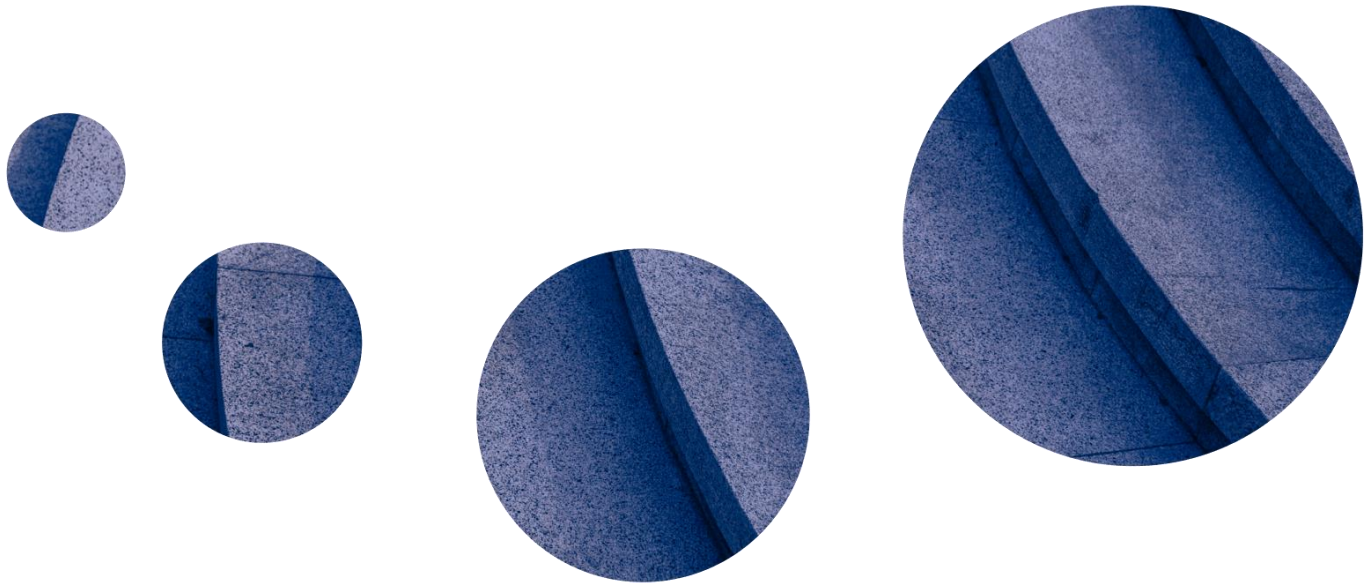




OBVERVIEW

Digital forensics is the process of using scientific concepts and procedures to examine electronical data which help to determine the steps of an event and therefore led to specific incident. It is important in this modern age of digital world for Digital Forensic professionals understand the technical scope to better prepared for the future. In past digital forensics were not known to be this dynamic. In the recent years several plan-of action, instrument and techniques are available dedicated for digital forensic principles. *“Digital forensics developed as an independent field in the late 1990s and early 2000s when computer-based crime started growing with the increasing usage of computers and more so, the Internet”* (Sriram Raghavan, 2013) The rapid Innovention of analysing and acquire digital evidence from Mutiple sources and tools has comes with challenges in the aspect multiple areas.

The history

The history of digital forensic can be traced back to Hans Gross (1847 -1915), who was the first to introduce scientific examination in criminal investigations. The FBI also played a significant role by establishing a lab in order to provide forensic assistance to law enforcement agencies. One of the earliest recognitions of computer crime occurred in 1978 through the Florida Computer Crime Act. Francis Galton (1882) (Holt, J, T., Bossler, M, A. and Seigfried-Spellar, C, K., 2015) conducted the initial documented investigation on fingerprints, while the term 'Computer Forensics' appeared in scholarly works for the first time in 1992. Subsequently, The International Organization on Computer Evidence was founded in 1995 and later, Regional Computer Forensic Laboratories were established by FBI starting from year 2000 onwards. In 2002, "Best practices for Digital Forensics" handbook was released by Scientific Working Group on Digital Evidence marking another milestone followed by Simson Garfinkel's emphasis on challenges faced during digital investigations in 2010. Overall, the field of digital forensics has a rich history and has evolved significantly over time to address the challenges posed by advances in technology and increasing sophistication of cybercrime. (Fyffe, G., 2008)

Introduction

The objective of this task is to carry out an investigation into digital forensics, covering the historical background of the field, its current status and its intersection with cybersecurity. Additionally, it will explore the evolving trends in digital forensics and cybersecurity along with a detailed examination of key challenges. Furthermore, an analysis of the national and international job market will be conducted. Investigation into Digital Forensics and Cybersecurity. As organisations continue to navigate the complex landscape of data security, the importance of digital forensics and cybersecurity has become increasingly evident. In this investigation, we will dive into the historical background of digital forensics, examining its roots and evolution in parallel with the advancement of technology and cyber threats. Furthermore, we will explore the status of digital forensics, shedding light on its intersection with cybersecurity. This includes delving into how digital forensics contributes to the proactive protection of digital assets and the investigation of security incidents.

Evolving trends in digital forensics and cybersecurity will also be a focal point of this investigation. With the rapid pace of technological advancement, it is essential to understand how these fields are adapting to new challenges and emerging threats. Moreover, a comprehensive examination of the challenges faced in digital forensics and cybersecurity will be conducted, providing insights into the obstacles that professionals and organisations encounter in these domains.

To conclude the investigation, an analysis of the national and international job market for digital forensics and cybersecurity will be presented, offering perspective on the demand for skilled professionals in these critical areas of information security.

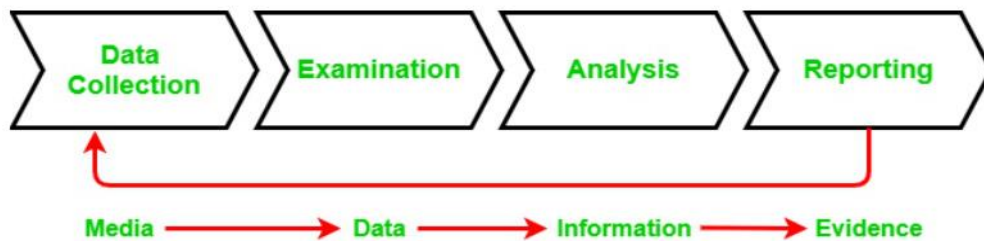
Current state of the field

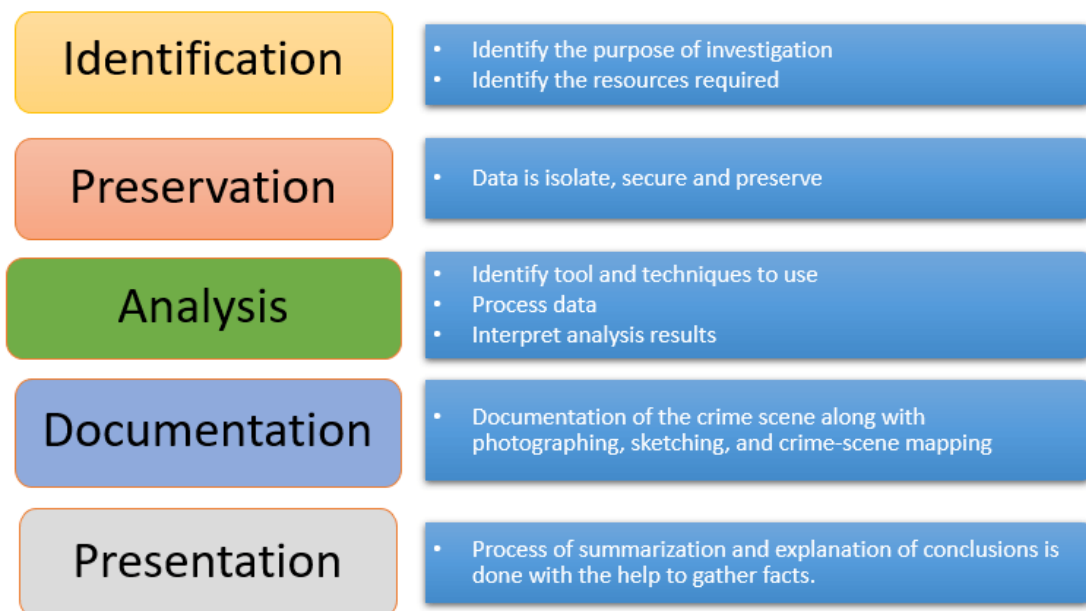
The current and future state of digital forensic requires more up-to-date tools to combat the ever-involving field. New tactics technique and technologies are needed to facilitate the identification, extraction, analysed and documentation of electronic evidence. As we can see in recent year, Fileless Malware, which is stealthy, have abilities to hide itself from detection and using anti-forensic techniques making it very hard for law and forensic investigators professionals. Zero-day vulnerabilities is another serious threat which can be exploited and not detected for weeks, month even years.

Supply Chain attacks is another challenge in the field since it involves third parties. Makes cybersecurity and digital forensic investigators work very difficult. The emerging of artificial intelligent (AI) and machine-learning (ML) are alternative and current opportunities trending in field. Yet, 2023 is changing the current and potential future digital forensic and incident response, ChatGPT is one of these examples. AI and machine learning are the shaping the way. Khaitan (2023) argued that Ashish Khaitan highlights the significant impact of these two technologies on digital forensics, emphasising their ability to enhance evidence collection and processing in real-time.

Furthermore, he notes that these technologies play a crucial role in revolutionizing network traffic analysis. Additionally, Khaitan suggests in the same article that ML algorithms, supported by Intrusion Detection Systems, can facilitate efficient real-time threat detection. (Ashish Khaitan, 2023) However, many other researchers believe that the maturity of these Technologies still needs more research to fully integrated into digital forensic and its sensitivities. Nevertheless, some argued that the effectiveness and accuracy of these Technologies on digital images and videos is priceless.

(Dwivedi et al) state that although these technologies offer various advantages and applications, there are also multiple risks associated with their use in digital forensic investigation. Adhering to specific guidelines is essential to maintain the chain of custody and ensure the admissibility of evidence in court. Law enforcement agencies need to thoroughly evaluate the maturity of these technologies. OpenAI recommends exercising caution when employing GPT-4 outputs, particularly in situations where reliability is crucial. In terms of cybersecurity, AI and machine learning play a significant role in identifying anomalies and suspicious activity for uncovering hidden attacks or indicators thereof.





Intersection of digital forensics and cybersecurity

Digital forensics is the result of cybercrime, occurring after a breach or criminal activity involving electronic devices. Cybersecurity involves preventing unauthorised access to data, and professionals in this field can utilize information from digital forensics to enhance future crime prevention efforts. Both disciplines share common tools and concentrate on safeguarding data - cybersecurity prevents breaches while digital forensics aids in recovering compromised data. The two disciplines, cybersecurity and digital forensics, complement each other in the realm of data protection (Holt, J, T., Bossler, et al 2015) In addition, the close collaboration between cybersecurity and digital forensics allows for a more comprehensive approach to addressing cybercrime (Chabot, Y. et al., 2015).

Digital forensics focuses on retrieving data from networks, systems, and devices for investigation to determine what took place and the extent of the damages. It also aims to detect the source of the incident and identify who is responsible. On the other hand, cybersecurity professionals are focused on protecting data from unauthorised access by using tools, policies, and strategies to secure networks and systems. Although their approaches may differ, collaboration between these two fields in threat intelligence and security strategies can be valuable for an organisation's future incident response planning and asset protection.

Incident Response and Investigation:

Cybersecurity Perspective: Cybersecurity involves implementing measures to prevent and respond to security incidents.

- ❖ *Digital Forensics Perspective*: Digital forensics is essential for investigating and analysing the aftermath of security incidents to understand their scope, impact, and identify the attackers.
- ❖ *Collection and Preservation of Evidence*:
- ❖ *Cybersecurity View*: The focus is on monitoring and preventing incidents in real-time.
- ❖ *Digital Forensics View*: Emphasizes the methodical gathering and preservation of digital evidence for future investigations and legal use.

Threat Intelligence:

- ❖ *Cybersecurity View*: Involves collecting and analysing information about potential threats.
- ❖ *Digital Forensics View*: Uses threat intelligence to improve the investigation process by understanding adversaries' tactics, techniques, and procedures.

Malware Analysis:

- ❖ *Cybersecurity View*: Aims to prevent and detect malware presence.
- ❖ *Digital Forensics View*: Involves analysing malware post-incident to comprehend its functionality and how it infiltrated systems.

Continuous Monitoring:

- ❖ *Cybersecurity Perspective*: Entails real-time network and system monitoring.
- ❖ *Digital Forensics Perspective*: Provides historical data for investigators to reconstruct events leading up to a security incident.

Forensic Readiness:

- ❖ *Cybersecurity Perspective*: Focuses on preparing systems for potential incidents.
- ❖ *Digital Forensics Perspective*: Concentrates on ensuring effective collection, preservation, and analysis of digital evidence when needed.

Legal Implications

- ❖ *Cybersecurity Perspective*: Stresses compliance with regulations & policies.
- ❖ *Digital Forensics Perspective*: Addresses the legal aspects of evidence collection making sure it's admissible in court

Training And Skillsets

- ❖ *Cybersecurity perspective* demands skills in intrusion detection vulnerability management threat prevention,
- ❖ *Digital forensic view* necessitates expertise in evident handling recovery forensic analysis
- ❖ *Collaboration*

- ❖ Cybersecurity Penselin focuses proactive po security measures, -Often comes ndently after instigative encounter but contributes to improving overall cybersecurity strategy.

Understanding and effectively managing the intersection of digital forensics and cybersecurity is crucial for developing comprehensive security strategies, improving incident response capabilities, and ensuring the resilience of digital systems against evolving cyber threats. Researchers in this area contribute to developing tools, frameworks, and best practices that bridge these two disciplines for a more robust cybersecurity

Emerging trends

With help of artificial intelligent, might need ways to analysed large data because during organised crime investigation, immense volume of devices will be analysed deferent technique is needed to pullout data from these devices. The amount of time this process will take is hug. Research has been conducted to find a generic method to export data and to determine if there is a 'common export format which would enable the various extract types to be merged for intelligence and evidence analysis purposes' (Quick, Choo, 2016).

The researchers examined different options to export data in a variety of formats from 'EnCase, FTK Imager, Cellebrite UFED, MSAB XRY, IEF, Oxygen, and Paraben'. As a result, a volume reduction was observed, from a total of 339.9 GB to 207.6 MB in spreadsheets (CSV, XLS, or XLSX), and to 485.4 MB for XML files, representing the exported and parsed data including contacts, calls, messages, emails, Gmail, web bookmarks, GPS coordinates, and a range of other application information' (Quick, Choo, 2016).

Mobile devices also are often a valuable source of evidence, as there is a wealth of potential data that can be recovered from them and improve investigation processes by contributing to intelligence analysis in terrorism, child exploitation, drug trafficking, homicide, fraud, computer crime, and other investigations. Even after deletion of data by the owner or third party, certain amount of information (including sensitive) can still be recovered (Blondel et al. 2015).

Key Challenges

According to David Lillis and colleagues, a report from Juniper Research in 2015 estimated that the number of IoT devices had reached 13.4 billion, with an expected increase to 38.5 billion by 2020 (MacDermott, Á. et al., 2020) These IoT devices include smart technologies such as smartphones, smart homes, and cars, which store data either in personal or manufacturer/retailer cloud spaces. As a result, the collection of data for investigations presents challenges.

The IoT has the potential to provide valuable evidence from the physical world; however, it also introduces unique difficulties for digital forensic investigators the field of digital forensics is currently more challenging than ever before. Therefore, no indications that this will change in the near future. The rise of Cloud Forensics and Internet of Things Forensics, coupled with the lack of standardization and restricted tools in the domain, as well as persistent case backlogs within digital forensics have significantly increased challenges for investigators. Storing data in the cloud across multiple devices globally means that investigators must navigate local laws and regulations when collecting evidence, unlike traditional methods where data is collected from a single computer or network. Cross-border investigations involving evidence located in multiple countries present countless unsolved cases due to regulatory frameworks governing access to electronic evidence. Ethical and legal procedures vary between countries regarding how to exchange such evidence, while anti-forensic techniques pose further challenges by disrupting forensic analysis efforts or damaging examination tools (Garfinkel S., 2007; Simson L., 2007).

Additionally, Advanced Persistent Threats and state-sponsored Malware introduce new challenges due to their sophisticated attack techniques. Rousseve indicates that creating an embedded help team for a forensic examiner may be one solution to effectively address these issues through global cooperation on laws and frameworks.

Forensic backlogs

The increasing accumulation of unresolved digital forensics cases poses a significant challenge for law enforcement agencies. This challenge extends beyond data collection to encompass the identification and analysis of time-consuming data. For example, a single cyber-crime investigation can yield hundreds of gigabytes of data, making the collection and analysis processes distinct and complex. Timely analysis of collected data presents considerable challenges. Simon Kempton, the technology lead for the Police Federation of England and Wales, emphasised that the consistent number of digital devices awaiting analysis compared to last year.

Reflects investigators. overwhelming workload due to the sheer volume of digital evidence. Law enforcement agencies are finding it difficult to recruit new detectives, resulting in mounting workloads. In 2022 alone, over 20,000 devices await examination in the UK while numerous tablets and smartphones also await inspection across the country

Scalability

This presents a critical issue in the field of digital forensics, particularly concerning scalability and its connection to the volume challenge in digital investigations. Examiners often encounter difficulties due to the quantity and complexity of metadata or sensitive information at a crime

scene. The increasing volume and complexity of data or systems, coupled with limited adoption of new technology by experts, contribute to this problem. Furthermore, there is an imbalance between cybercrime incidents and available examiners in the industry, necessitating thorough investigation by every expert. Without adequate resources and efficient processes, digital forensic investigations may struggle to keep up with the growing volume of data and devices that need examination (Cahyani, W, D, N. et al., 2017)

National and International Job Market

The Landscape of Digital Forensics Employment in the United Kingdom

The United Kingdom's job market in digital forensics is a dynamic and evolving landscape, reflecting the increasing importance of cybersecurity in various sectors. This we explore key aspects of the UK job market in digital forensics, shedding light on demand, industry sectors, qualifications, government influence, and networking opportunities.

Demand for Digital Forensics Professionals: The demand for digital forensics professionals in. As cyber threats become more sophisticated, organisations across industries are recognising the need for skilled experts capable of investigating and mitigating cyber incidents. This demand is particularly pronounced in sectors such as law enforcement, government agencies, financial institutions, and cybersecurity firms. (Prospects.ac.uk, 2023)

Key Industries and Sectors: Digital forensics expertise is sought after in various industries in the UK. Law enforcement agencies leverage digital forensics to investigate cybercrimes, while government organizations prioritize securing sensitive information. Financial institutions engage digital forensics professionals to combat financial fraud, and cybersecurity firms rely on their skills to fortify defences against cyber threats. The private sector, including corporations of all sizes, increasingly integrates digital forensics into risk management and incident response strategies.

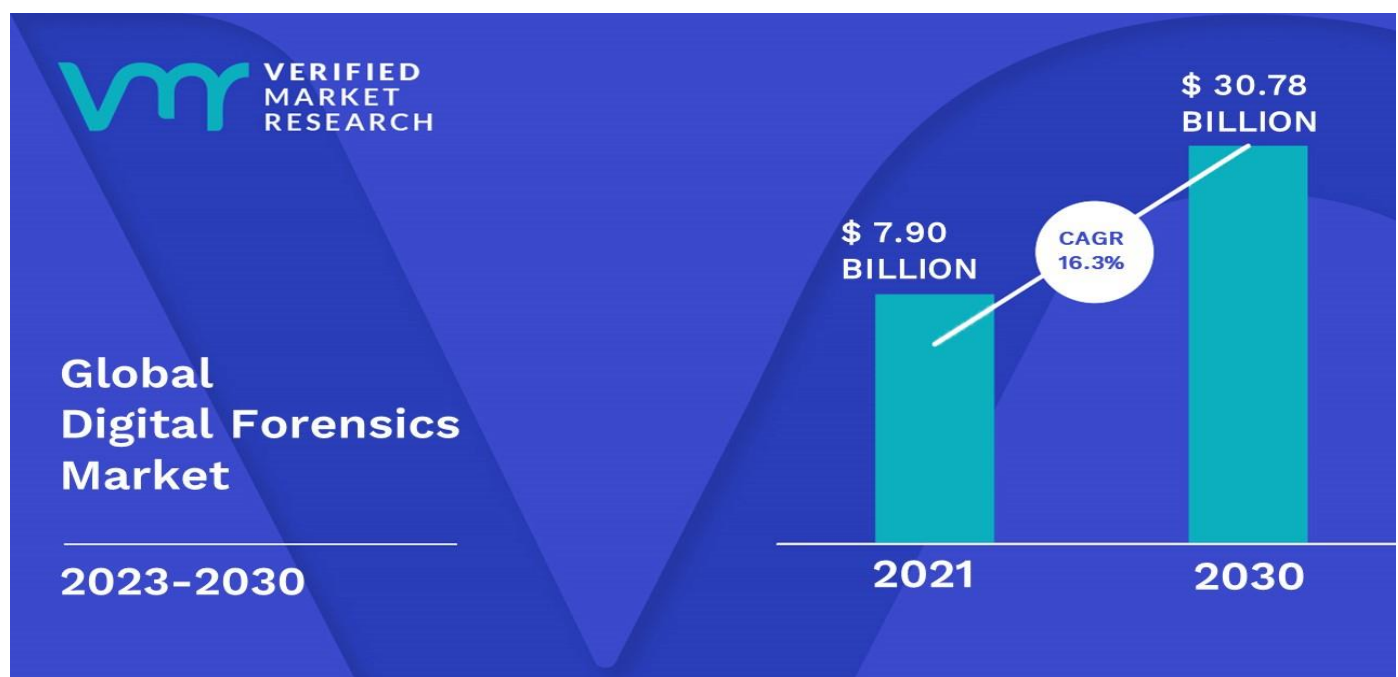
Qualifications and Certifications: In the competitive UK job market, qualifications and certifications play a pivotal role. Employers often seek candidates with relevant academic backgrounds, such as degrees in cybersecurity, computer science, or digital forensics. Certifications like Certified Digital Forensics Examiner (CDFE), Certified Cyber Forensics Professional (CCFP), and others are highly regarded, providing tangible evidence of practical skills and knowledge. (Tully, G. et al., 2020)

Government Initiatives and Regulations: The UK government's commitment to cybersecurity is reflected in various initiatives that influence the job market. National cybersecurity strategies and collaborations between public and private sectors create an environment conducive to the growth of digital forensics roles. Compliance with government regulations and adherence to legal frameworks are crucial aspects of digital forensics work, adding a layer of complexity to the profession.

Networking Opportunities: Networking is a key element in navigating the digital forensics job market. Professionals in the UK can engage in networking events, conferences, and industry-specific meetups to build connections. Online platforms like LinkedIn provide avenues for virtual networking, allowing individuals to stay informed about industry trends, job openings, and collaborative opportunities.

The United Kingdom's job market in digital forensics presents a promising landscape for professionals in the cybersecurity domain. With a growing demand for expertise, particularly in law enforcement, government, finance, and the private sector, individuals equipped with the right qualifications and certifications can carve out successful careers. Government initiatives, coupled with a proactive approach to networking, contribute to the resilience and adaptability required in this fast-paced field. As technology continues to advance, the role of digital forensics professionals

report titled "Global Digital Forensics Market 2018 - 2025" projects that the digital forensics market is expected to reach \$7 billion by 2025, a significant increase from the reported \$3 billion in 2017. With an expanding reliance on connected devices by both companies and general consumers, the risk of falling victim to cybercrime has also grown. (Du, X. et al., 2020) The study suggests that approximately half of the world's population engages with some form of digital device daily. As the global population grows and technology becomes more accessible at lower costs, it is anticipated that cybercrime will rise, presenting new challenges for security professionals. Encouragingly, there are several emerging technologies showing promise in assisting digital forensic investigators. Safeguarding digital assets and conducting investigations into cyber incidents are expected to play an increasingly important role in the UK job market. As technology continues to advance and cybercrime becomes more prevalent, the need for highly skilled and knowledgeable digital forensics professionals will only grow (Naqvi, S., Sommer, P. and Josephs, B, M., 2019).



Open-source vs Commercial forensic tools, review

In the context of forensic tools typically refer to methods or procedures for analysing and examining evidence in criminal investigations. Forensic tools, whether open-source or commercial, are essential for digital forensics, which involves the collection, analysis, and preservation of electronic evidence. Here's a comparison between open-source and commercial forensic tools:

Open-Source Forensic Tools:

Documentation on open-source tools may not be as thorough or intuitive as the documentation available for commercial tools. Additionally, certain open-source tools may have limited integration with other forensic tools and lack the seamless interoperability provided by commercial solutions. In conclusion, open-source digital forensic tools offer cost savings, community support, transparency, and customization options (Holt, J, T. et al 2015)

Commercial Forensic Tools:

User-Friendly Interfaces: Many commercial tools feature interfaces that are easy for investigators with different levels of technical knowledge to use.

Comprehensive Support: Commercial tools typically provide thorough technical support, including updates, bug fixes, and training resources. This can be crucial for organizations needing reliable and current solutions.

Integration: Numerous commercial forensic tools are developed to seamlessly integrate with other platforms and tools, streamlining workflow efficiency.

Advanced Features: Commercial tools often come equipped with advanced capabilities not found in open-source alternatives. These features can be particularly useful when dealing with intricate forensic investigations.

Cost Consideration: The main drawback of commercial tools is the associated cost for licensing and support services. This may present a barrier for smaller organizations or individuals on limited budgets.

Closed Source Issue: Commercial tools tend to be proprietary, withholding their source code from inspection. Some users may have concerns about trust and security due to this lack of transparency

Users who rely on commercial software require ongoing support from the vendor, which includes updates and bug fixes. If this support is discontinued, it can create difficulties for users. The decision to use open-source or commercial forensics tools depends on factors such as budget, user expertise, specific case requirements, and level of support needed. Some organizations may

opt to utilize a combination of both types of tools in order to leverage the advantages offered by each option.

Ultimately, choosing between open-source and commercial digital forensics tools involves considering various factors like budget limitations, user proficiency, and specific case needs. (Abulaish, M. and Haldar, H, A, N., 2018) Digital forensics has evolved significantly over time, with various milestones and advancements marking its progress (Holt, J, T., Bossler, M, A. and Seigfried-Spellar, C, K., 2015). These milestones include the establishment of forensic labs by the FBI, the recognition of computer crime acts, and the founding of organizations such as The International Organization on Computer Evidence. Additionally, the release of handbooks and publications, such as the "Best practices for Digital Forensics," have provided valuable guidance to practitioners in the field (Raghavan, V, S., 2012)

Conclusion

In conclusion, the field of digital forensics has a rich history that dates to the 19th century and has evolved significantly over time to address the challenges posed by advances in technology and the increasing sophistication of cybercrime. (Holt, J, T., Bossler, M, A. and Seigfried-Spellar, C, K., 2015) This evolution has led to the establishment of international organisations, the development of forensic tools, and the recognition of digital evidence across various devices.

Furthermore, the emergence of peer-reviewed journals and training programs has contributed to the growth of knowledge and expertise in the field. As technology continues to advance and criminals find new ways to exploit digital devices, the field of digital forensics will continue to adapt and evolve to stay one step ahead in identifying and combating cybercrime. In conclusion, the field of digital forensics has a rich history that dates to the 19th century and has evolved significantly over time to address the challenges posed by advances in technology and the increasing sophistication of cybercrime.

This evolution has led to the establishment of international organizations, the development of forensic tools, and the recognition of digital evidence across various devices. Furthermore, the field continues to advance with ongoing research and development, as well as the collaboration between academia, law enforcement agencies, and industry professionals. Overall, the field of digital

forensics has come a long way and continues to make strides in its ability to investigate and analyse digital evidence

Activity 2

The Sleuth Kit and Autopsy stand out as widely recognized forensic toolkits. The Sleuth Kit is a command-line utility for analysing forensic images of hard drives and mobile devices, while Autopsy provides a GUI-based interface that utilizes The Sleuth Kit in the background. Both toolkits feature a modular design with plug-in capabilities, allowing users to seamlessly integrate additional functionality. These tools are open source, but also offer commercial support and training services. They are suitable and widely used for digital forensic investigations on various operating systems, including Windows, Linux, OS X, and other Unix platforms

Image creation: FTK imager

Autopsy and The Sleuth Kit are designed for examining disk images of hard drives, smartphones, and other devices. Analysing an image instead of a live drive allows the investigator to demonstrate that no modifications have been made to the drive that could impact forensic results.

Autopsy does not include image creation capabilities, so another tool must be utilized. Although most items in the Access Data Forensics Toolkit are paid tools, its FTK Imager is available as a free product. This tool can be used to create disk images for subsequent analysis with Autopsy/The Sleuth Kit.

Memory forensics: Volatility

Tools such as The Sleuth Kit primarily target the hard drive, yet forensic data and artifacts may also be found in other areas of a computer. Crucial forensic information can reside in RAM, requiring swift and meticulous collection to ensure its validity and usefulness for investigations.

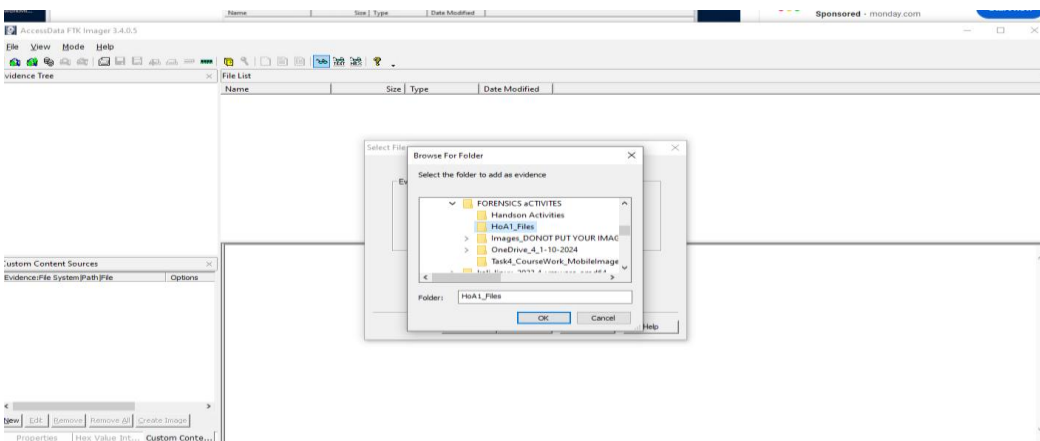
Volatility is widely recognised as the leading tool for analysing volatile memory. Like The Sleuth Kit, Volatility is open-source, free of charge, and compatible with third-party plugins. Additionally, the Volatility Foundation organises an annual competition for users to create valuable and innovative extensions for the framework.

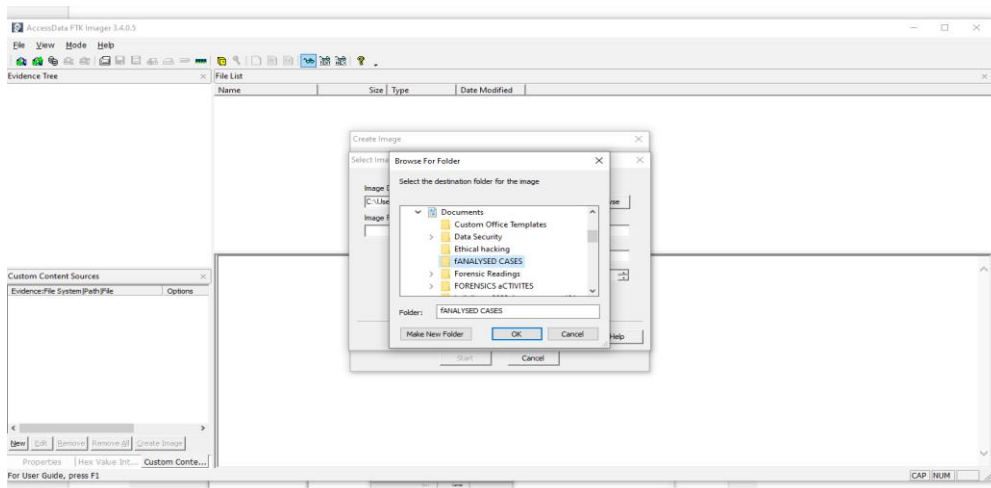
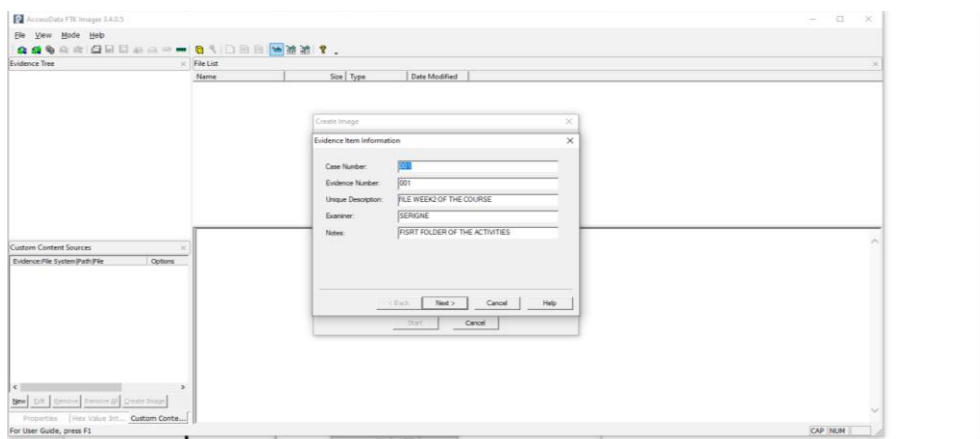
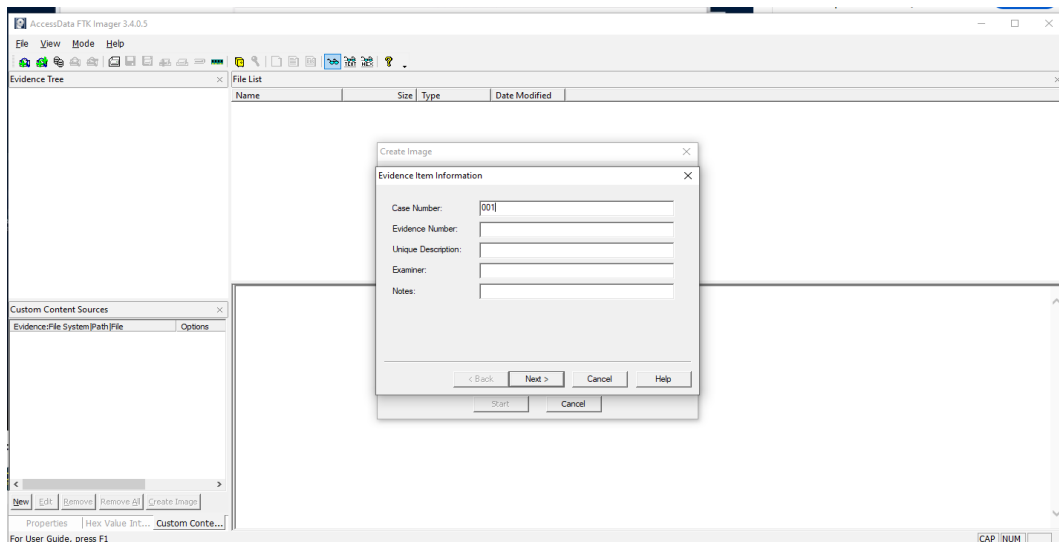
Mobile forensics: Cellebrite UFED

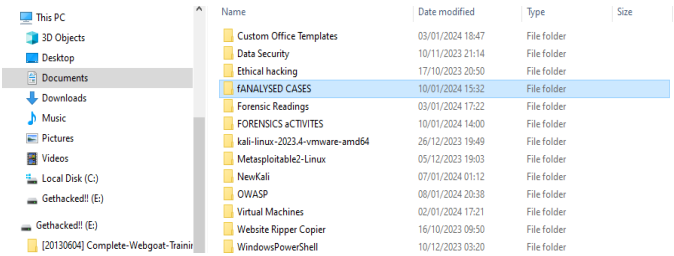
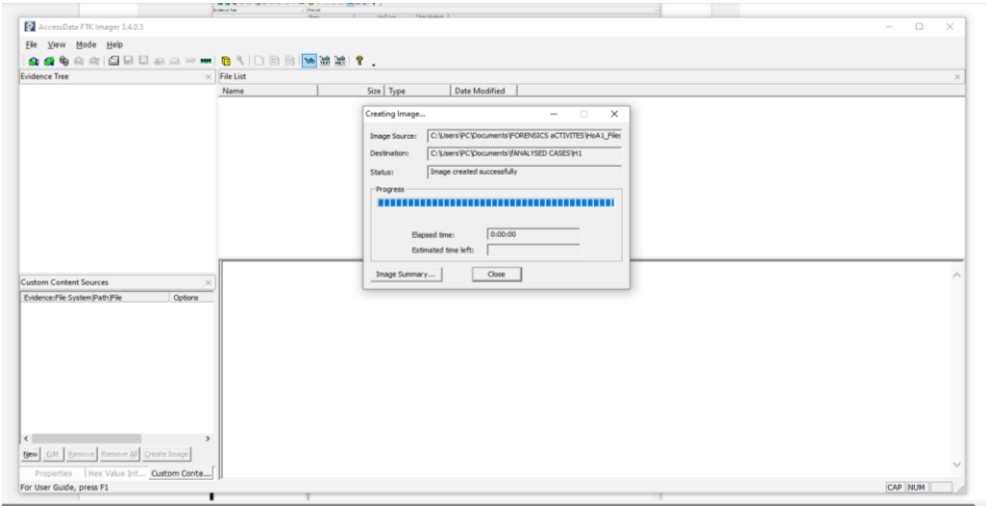
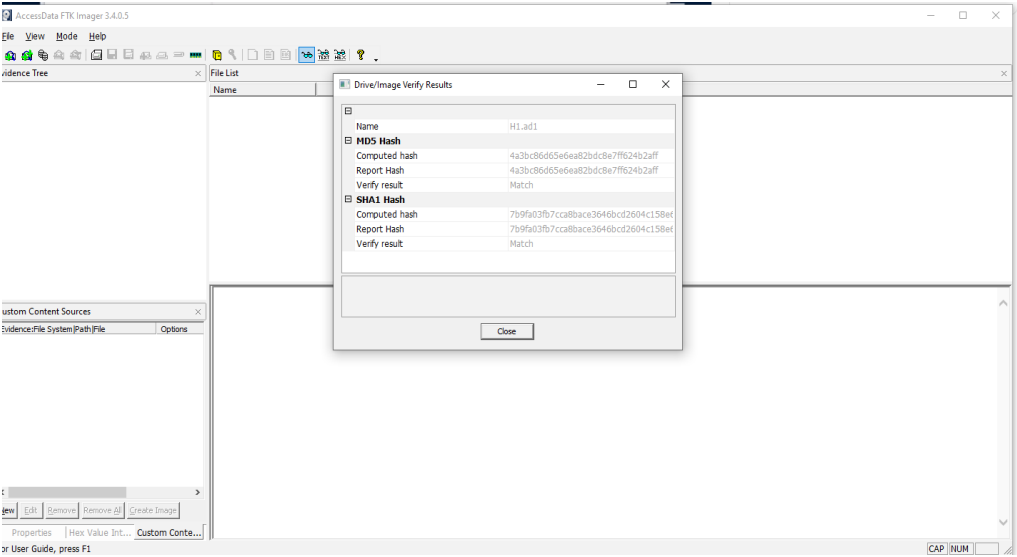
The prevalence of mobile devices in work environments is on the rise due to growing technological needs. This has led to an increase in cyberattacks such as phishing, which can potentially access valuable forensic data stored on these devices. As mobile forensics becomes more important, obtaining a specialized tool that focuses on analysing mobile devices could be advantageous. Cellebrite UFED is acknowledged as a top commercial solution for mobile forensics because it supports various platforms beyond just mobile devices and offers exclusive methodologies and tools specifically designed for analysing such devices.

Network analysis: Wireshark

Numerous forensic tools focus on the endpoint, but there are also significant data sources to consider in a forensic inquiry. Most cyberattacks occur over the network, and scrutinising network traffic captures can help in identifying malware and retrieving data that may have been removed or replaced on the endpoint. Wireshark is widely acknowledged as the main tool for analysing network traffic, providing dissectors for different kinds of network traffic along with a user-friendly GUI for analysis and comprehensive underlying features. It supports live capture and examination of captured network files.







ents > ANALYSED CASES

▼ 🔍 Search ANALYSED CASES P

Name	Date modified	Type	Size
 HT.ad1	10/01/2024 15:32	AD1 File	346 KB
 HT.ad1	10/01/2024 15:32	Text Document	1 KB

References

(Abel Yeboah-Ofori's, 2022) *For digital evidence to appear at court and be legally admissible, the evidence must be authentic, accurate, complete, and convincing to the jury.*
https://www.researchgate.net/publication/342706049_Digital_Forensics_Investigation_Jurisprudence_Issues_Of_Admissibility_Of_Digital_Evidence#fullTextFileContent (Accessed 24 December 2023)

Mohammed I. Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities Alghamdi (202) Available file:///C:/Users/PC/Downloads/Digital_Forensics_in_Cyber_Security-Recent_Trends_.pdf: (Accessed 22 December 2023)

Top 5 Trends for Digital Forensics in 2023 Available: <https://thecyberexpress.com/top-5-trends-for-digital-forensics-in-2023/>: (Accessed 12 December 2023)

Ashish Khaitan (2023) Digital forensics is critical in investigating and prosecuting digital crimes and protecting organisations and individuals from cyber threats Available
: <https://www.marketsandmarkets.com/Market-Reports/digital-forensics-market-230663168.html>: (Accessed 27 December 2023)

Forensic computer analyst job profile | Prospects.ac.uk (2023). Available at:
<https://www.prospects.ac.uk/job-profiles/forensic-computer-analyst>. (Accessed 25 December 2023)

Naqvi, S., Sommer, P. and Josephs, B, M. (2019) A Research-Led Practice-Driven Digital Forensic Curriculum to Train Next Generation of Cyber Firefighters. Available at:
<https://doi.org/10.1109/educon.2019.8725129>. (Accessed 25 December 2023)

Holt, J, T., Bossler, M, A. and Seigfried-Spellar, C, K. (2015) Cybercrime and Digital Forensics: An Introduction. Available at: <https://ci.nii.ac.jp/ncid/BB18203417>. (Accessed 22 December 2023)

Mouhtaropoulos, A., Li, C. and Grobler, M. (2012) Proactive Digital Forensics: The Ever-Increasing Need for Standardization. Available at: <https://doi.org/10.1109/eisic.2012.66>. (Accessed 21 December 2023)

Chabot, Y. et al. (2015) Event Reconstruction. Available at: <https://scite.ai/reports/10.4018/978-1-4666-6324-4.ch015>. (Accessed 20 December 2023)

Johnston, C, A. (2022) A closer look at organizational cybersecurity research trending topics and limitations. Available at: <https://scite.ai/reports/10.1108/ocj-07-2022-0013>. (Accessed 07 December 2023)

Kuka, E. (2018) AN ANALYTICAL STUDY OF INFORMATION SECURITY MANAGEMENT IN THE PUBLIC SECTOR OF ALBANIA. Available at: <https://scite.ai/reports/10.12955/cbup.v6.1169>. (Accessed 17 December 2023)

Jordan, E. (1999) IT contingency planning: management roles. Available at: <https://scite.ai/reports/10.1108/09685229910292853>. (Accessed 21 December 2023)

Wiboonrat, M. (2008) An empirical IT contingency planning model for disaster recovery strategy selection. Available at: <https://scite.ai/reports/10.1109/iemce.2008.4617953>. (Accessed 17 December 2023)

Bartock, M. et al. (2016) Guide for cybersecurity event recovery. Available at: <https://scite.ai/reports/10.6028/nist.sp.800-184>. (Accessed 13 December 2023)

Fyffe, G. (2008) "Managing multinational compliance efforts while addressing corporate security needs," Network Security, 2008(4), p. 16-18. Available at: [https://doi.org/10.1016/s1353-4858\(08\)70054-0](https://doi.org/10.1016/s1353-4858(08)70054-0). (Accessed 23 December 2023)

C. Beek, T. Dunton, S. Grobman, M. Karlton, N. Minihane, C. Palm, et al., McAfee Threat Report, June 2018 Cyber Crime Costs Projected to Reach \$2 trillion by 2019, [online] Available: (Accessed 23 December 2023)

<https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/>. Cyber Crime Costs Projected to Reach \$2 trillion by 2019, [online] Available: <https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/>. (Accessed 23 December 2023)

Kristina V Statista (2016). Most popular global mobile messenger apps as of April 2016, based on number of monthly active users (in millions). Retrieved from: <http://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>. (Accessed 03 December 2023)

Available:<https://ieeexplore.ieee.org/document/6641058?denied=> Accessed 12 December (2023 November 2023)

Toby Marriott on February 6, 2023, Available at:[://www.adfsolutions.com/news/how-to-combat-the-uks-growing-forensics-backlog#:~:text=For%20example%2C%20a%20single%20cyber,prosecution's%20case%20against%20the%20offender.](http://www.adfsolutions.com/news/how-to-combat-the-uks-growing-forensics-backlog#:~:text=For%20example%2C%20a%20single%20cyber,prosecution's%20case%20against%20the%20offender.) (Accessed 23 December 2023)

Albert Robinson (2023) HOW DEVICE BACKLOGS AND LACK OF DIGITAL FORENSIC EXPERTISE ARE CAUSING LAW ENFORCEMENT TO OUTSOURCE DIGITAL FORENSICS How Device Backlogs and Lack of Digital Forensic Expertise are Causing Law Enforcement to Outsource Digital Forensics October (Accessed 12 December 2023)

Medha Mehta <https://cellebrite.com/en/how-device-backlogs-and-lack-of-digital-forensic-expertise-is-causing-law-enforcement-to-outsource-digital-forensics/> (Accessed 23 December 2023)

Estrela, V. & Estrela, Vania & Kanna, Kavita & Rodrigues, Joel & Rodrigues, Joel. (2021). Cybersecurity and Digital Forensics. Download citation of Cybersecurity and Digital Forensics (researchgate.net) <https://www.geeksforgeeks.org/digital-evidence-collection-in-cybersecurity/> (Accessed 13 December 2023)

Digital Forensics Market Size, Current Insights and Demographic Trends 2023-2031:<https://www.linkedin.com/pulse/digital-forensics-market-size-current>

Digital Forensics Market Size, Current Insights and Demographic Trends 2023-2031:<https://www.computer.org/csdl/magazine/sp/2017/06/msp2017060010/13rUx0xPSh>; Available:https://link.springer.com/chapter/10.1007/978-3-031-40118-3_8

Digital forensic research: current state of the art [Digital forensic research: current state of the art](#) | [CSI Transactions on ICT \(springer.com\)](#)

M. Vangeti, S. K. Yadav and V. Pinnti, “*Advantages of Internet of Things (IoT) For Developing Smart Services in Manufacturing Business*,” Purakala with ISSN 0971-2143 is an UGC CARE Journal, vol. 31, no. 25, pp. 62-68, (2020).

] O. M. Adedayo, “*Big data and digital forensics.*,” In 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF). IEEE., pp. 1-7, (2016).

] S. Raghavan, “*Digital forensic research: current state of the art.*,” CSI Transactions on ICT, vol. 1, no. 1, pp. 91-114, (2013)

E. A. Vincze, “*Challenges in digital forensics. Police Practice and Research*,” vol. 17, no. 2, pp. 183-194, (2016).

European Union Agency for Criminal Justice Cooperation. Detailed description in Cybercrime Judicial Monitor n.6. https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/cybercrime_judicial_monitor_issue_6_2021.pdf.

<https://www.sciencedirect.com/science/article/pii/S266628172300121X>

ChatGPT for digital forensic investigation: The good, the bad, and the unknown

W.J. Buchanan URL:<https://asecuritysite.com/forensics> (2023) Google Scholar CVE, 2014

CVE record | CVE-2014-0160 URL:<https://www.cve.org/CVERecord?id=CVE-2014-0160> (2014)
Google Scholar

Proceedings of Annual Conference of the North American Chapter of the Association for Computational Linguistics, NAACL-HLT) (2019), pp. 4171-4186

Du et al., 2021 X. Du, C. Hargreaves, J. Sheppard, M. Scanlon

TraceGen: user activity emulation for digital forensic test image generation

Forensic Sci. Int.: Digit. Invest., 38 (2021), Article 301133,

Scanlon et al., 2023 M. Scanlon, B. Nikkel, Z. Gerads

Digital forensic investigation in the age of ChatGPT

Forensic Sci. Int.: Digit. Invest., 44 (2023), Article 301543,

Thorp, 2023 H.H. Thorp ChatGPT is fun, but not an author

Science, 379 (6630) (2023), 10.1126/science. adg7879

313–313

tryhackme.com/room/introdigitalforensics

displays various metadata related to a PDF file, such as title, subject, author, creator, and creation date. (The AttackBox already has `pdftinfo` installed; however, if you are using Kali Linux and don't have `pdftinfo` installed, you can install it using `sudo apt install poppler-utils`.) Consider the following example of using `pdftinfo DOCUMENT.pdf`.

```
user@TryHackMe$ pdftinfo DOCUMENT.pdf
Creator:      Microsoft® Word for Office
365
Producer:     Microsoft® Word for Office
365
CreationDate: Wed Oct 10 21:47:53 2018
EEST
ModDate:      Wed Oct 10 21:47:53 2018
EEST
Tagged:       yes
UserProperties: no
Suspects:     no
Form:         none
JavaScript:   no
Pages:        20
```

THM AttackBox 52m 07s

20:26 03/01/2024

```
root@ip-10-10-125-65: ~/Rooms/introdigitalforensics
File Edit View Search Terminal Help
root@ip-10-10-125-65:~# cd /root/rooms
bash: cd: /root/rooms: No such file or directory
root@ip-10-10-125-65:~# cd /root/Rooms
root@ip-10-10-125-65:~/Rooms# cd intro
introdigitalforensics/ introloganalysis/
root@ip-10-10-125-65:~/Rooms# cd introdigitalforensics/
root@ip-10-10-125-65:~/Rooms/introdigitalforensics# ls
letter-image.jpg  ransom-letter.pdf
ransom-letter.doc  ransom-letter-2.zip
root@ip-10-10-125-65:~/Rooms/introdigitalforensics# ls
letter-image.jpg  ransom-letter.pdf
ransom-letter.doc  ransom-letter-2.zip
root@ip-10-10-125-65:~/Rooms/introdigitalforensics#
```

tryhackme.com/room/introdigitalforensics

containing the case files.

```
root# cd /root/Rooms
root# cd introdigitalforensics
root# ls
letter-image.jpg  ransom-letter.doc
ransom-letter.pdf  ransom-lettter-2.zip
```

Document Metadata

When you create a text file, **TXT**, some metadata gets saved by the Operating System, such as file creation date and last modification date. However, much information gets kept within the file's metadata when you use a more advanced editor, such as MS Word. There are various ways to read the file metadata; you might open them within their official viewer/editor or use a suitable forensic tool. Note that exporting the file to other formats, such as **PDF**, would maintain most of the metadata of the original document, depending on the PDF writer used.

Let's see what we can learn from the PDF file. We can try to read the metadata using the program **pdftinfo**. Pdftinfo displays various metadata related to a PDF file, such as

```
root@ip-10-10-125-65: ~/Rooms/introdigitalforensics# ls
letter-image.jpg  ransom-letter.pdf
ransom-letter.doc  ransom-lettter-2.zip
root@ip-10-10-125-65: ~/Rooms/introdigitalforensics#
```

THM AttackBox 49m 49s

20:28 03/01/2024