Digital Forensic Investigation

Dejuan Green
Norfolk State University

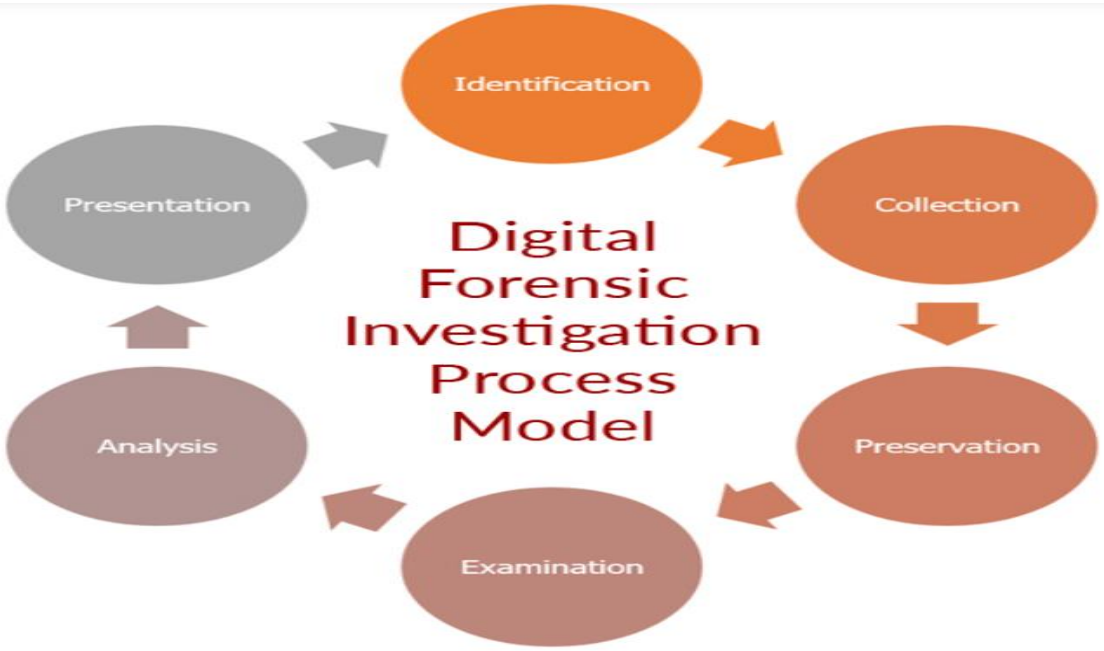
Dejuan Green

Digital forensic Investigation

Norfolk State University

Finding, acquiring, processing, analyzing, and reporting data on electronically stored data is the main goal of the forensic science discipline known as "digital forensics." Nearly all illegal acts include the use of electronic evidence, making digital forensics support essential for law enforcement investigations. Furthermore, digital forensics is very important to cases aiding in many cases and can lead to saving lives/ victims and locking up criminals. A wide range of devices, including laptops, cellphones, remote storage, unmanned aerial systems, shipborne equipment, and more, can be used to gather electronic evidence. [2] Digital forensics' major objective is to take data from electronic evidence, turn it into usable information, and then report the results to the police. All procedures make use of reliable forensic methods to guarantee that the information is acceptable in court.

It takes a lot of time to do digital forensics. To begin with, detectives search for evidence on technological devices and store the information to a secure disc. After that, they examine and record the data. When it's prepared, they hand over the digital evidence to the police to aid in a crime's investigation or show it in court to aid in a criminal's conviction. Nine stages are often followed by digital forensic professionals when examining digital evidence, according to my study. A digital forensic team initiates the first response as soon as a security event happens and is reported [4]. The team then searches crime-related devices for data and evidence during search and seizure. Following the seizure of the devices, experts gather the data utilizing forensic techniques to manage the evidence. [4] The fourth step is evidence security, in which investigators keep evidence in a secure location. The data may be verified as legitimate, accurate, and available in a secure setting. The forensic team immediately follows data acquisition by retrieving electronically stored information (ESI) from the devices. Professionals must follow the right processes and take caution to prevent data manipulation and loss of the validity of the evidence. To find and prepare material that will be valuable in court, members of the Data Analysis Team first sort and review the authenticated ESI. Investigators evaluate ESI once it has been recognized as evidence considering the security incident. In this stage, the information acquired will be directly related to the case. After the preliminary criminal investigation is complete, documentation and reporting take place. Members of the team compile data and evidence and report it in compliance with legal standards. Finally, expert witness testimony is provided by a specialist who has knowledge of the subject matter of the case. The data is presented in court by the expert witness, who declares it appropriate for use as evidence. This workflow model was presented to me by a digital forensics business as well.



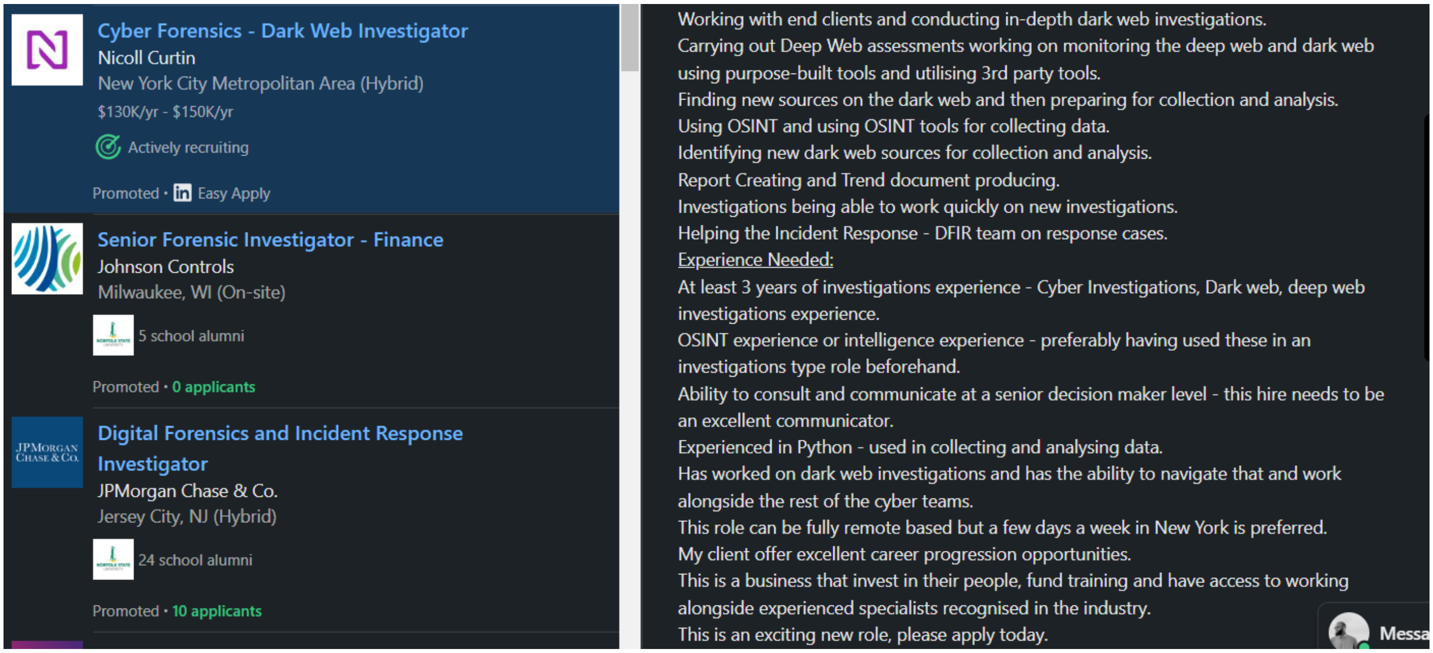
[1]

Practically all of the steps in digital forensics are performed on electronic devices, the forensic team needs the best software available. The products and procedures listed below assist digital investigators in finding data lawfully and securely extracting it. With the help of the Sleuth Kit, forensic experts may access a C library, use a set of command-line tools, examine disk images, and recover files. [3] With Volatility, forensic experts can quickly list the kernel modules on an 80G B system, look into virtual machines, and use a web interface that can be customized. [3] With the help of the Cellebrite UFED (Universal Forensic Extraction Device), forensic experts may use data collecting tools in the field, at a remote location, and in the lab.; to bypass password/PIN locks on mobile devices and access cloud tokens and app data. [3]To utilize numerous services that enable remote authentication, browse a list of supported services for brute-forcing, and save a service module as a.mod file, forensic professionals can use Medusa. [3] The utilization of distributed cracking networks, automated performance adjustment, and testing of several device kinds on a single machine are all made possible by Hashcat for forensic professionals. [3] Online inspection enables forensic professionals to employ centralized program management tools, perform simultaneous crawl testing at multiple skill levels, from expert to novice, and test the dynamic behavior of web applications for security flaws.

The tools are only part of the solution. Additionally, forensic investigators must be trained in its appropriate usage. Combating anti-forensic tactics, comprehending system forensics, accessing file systems and hard drives, and looking into email crimes are all necessary talents. [4] Obtaining credentials might be advantageous for these professionals as well. One of the foundational certs that most people have in the cyber work field is the CompTia A+. One well-known certification in the industry is Global Information Assurance Certification (GIAC), which offers programs like GIAC Certified Forensic Examiner and GIAC Response and Industrial Defense. [4] A forensic investigator's profession can be advanced by taking courses and earning certifications from organizations like AccessData and the International Association of Computer Investigative Specialists. [3]

Once you have the skills and the certification in cyber forensics there are a lot of places you can work. I know that the FBI has teams of cyber forensics to aid them on cases and in many cases, they aid in saving many people's lives. If you would like to work in Virginia, I have seen a number of job postings in the Chantilly area. If you have gotten comfortable staying at home after covid I have found remote options as well that were listed on google as well. Cyber forensics is a broad field so if the digital investigation track doesn't quite interest you there will be something that will.

Below is a snippet from my linked-in which shows available jobs in this field as well as the role and requirements for the first job listed.



Cyber Forensics - Dark Web Investigator
Nicoll Curtin
New York City Metropolitan Area (Hybrid)
$130K/yr - $150K/yr
Actively recruiting
Promoted · Easy Apply

Senior Forensic Investigator - Finance
Johnson Controls
Milwaukee, WI (On-site)
5 school alumni
Promoted · 0 applicants

Digital Forensics and Incident Response Investigator
JPMorgan Chase & Co.
Jersey City, NJ (Hybrid)
24 school alumni
Promoted · 10 applicants

Working with end clients and conducting in-depth dark web investigations.
Carrying out Deep Web assessments working on monitoring the deep web and dark web using purpose-built tools and utilising 3rd party tools.
Finding new sources on the dark web and then preparing for collection and analysis.
Using OSINT and using OSINT tools for collecting data.
Identifying new dark web sources for collection and analysis.
Report Creating and Trend document producing.
Investigations being able to work quickly on new investigations.
Helping the Incident Response - DFIR team on response cases.
Experience Needed:
At least 3 years of investigations experience - Cyber Investigations, Dark web, deep web investigations experience.
OSINT experience or intelligence experience - preferably having used these in an investigations type role beforehand.
Ability to consult and communicate at a senior decision maker level - this hire needs to be an excellent communicator.
Experienced in Python - used in collecting and analysing data.
Has worked on dark web investigations and has the ability to navigate that and work alongside the rest of the cyber teams.
This role can be fully remote based but a few days a week in New York is preferred.
My client offer excellent career progression opportunities.
This is a business that invest in their people, fund training and have access to working alongside experienced specialists recognised in the industry.
This is an exciting new role, please apply today.

References

[1] “Digital Forensic Investigation – BHF | BLACKHAT FORCE (PVT) LTD.” https://blackhatforce.com/main/forensic-investigation/ (accessed Oct. 20, 2022).

[2]“Digital forensics,” www.interpol.int. https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch (accessed Oct. 23, 2022).

[3]“Digital Investigation – Top Tech Search Reviews | Find Company in your Location.” https://toptechsearch.com/listing/digital-investigation/?utm_source=google&utm_term=cyber%20forensic%20investigation&gclid=CjwKCAjwzNOaBhAcEiwAD7Tb6FQC9jmfVhp0JLyTStCLRRG1hTOnM6zwrRyVR5oSZRhyqIAO2u10OxoCAX4QAvD_BwE (accessed Oct.23, 2022).

[4] “The Phases of Digital Forensics,” University of Nevada, Reno, Oct. 01, 2021. https://onlinedegrees.unr.edu/blog/digital-forensics/#:~:text=The%20Digital%20Forensic%20Process (accessed Oct.23, 2022).