

Cyber Security & Demand for Digital Forensics

@Forensichima

<http://linkedin.com/company/CyberPsy>

<https://www.linkedin.com/in/forensichima/>

<https://www.facebook.com/groups/cyberpsy>

Instagram : Himaveeramachaneni



CYBERPSY



Disclaimer - 'The views and opinions expressed are my personal and do not reflect my employer opinions', this is voluntary talk to contribute to the community

@Forensichima



CYBERPSY

Hima Bindu Veeramachaneni

- ❖ **Founding Member of CyberPsy , Global community Initiative**
- ❖ NASSCOM Hackathon Winner, Mentor, Coach, Author, Speaker, Toastmaster (CC CL), Technology Evangelist
- ❖ HYSEA Women Hackathon Special Jury Award Winner
- ❖ Expertise in Security Space, working as Sr. Manager Leading EnCase Forensics and Security
- ❖ **Global Speaker** - at various technical events and communities, Women Tech\Global, Cyberjutsucon, StartupImpactSummit , WHackzcon, CyberSecCareerConference
- ❖ Governing Body Member of Gudlavalleru Engineering College
- ❖ Recognized as Lady Legend, MVP Awardee 8 times in a row, Ex -Microsoftee
- ❖ Data Security Council of India (DSCI) Hyderabad - Core Member
- ❖ Author at PC Quest, Simple-Talk, ASP Alliance, Code Project
- ❖ Mentor at Executive Womens Forum and Global CyberSecurity Mentorship Program
- ❖ **Guinness Book World Record Holder - Microsoft APP Fest Windows8 Hackathon**
- ❖ Volunteer in Girls in Tech, Workwayinfo, Ambassador for DevOpsInstitute and WomenTechNetwork



@Forensichima



<https://www.linkedin.com/in/forensichima>



CYBERPSY

Agenda

- ❖ What is Digital Forensics?
- ❖ Skills Required
- ❖ History and Evolution
- ❖ Types of Forensics
- ❖ Benefits and Use Cases
- ❖ Opportunities
- ❖ How to Get Started
- ❖ Certifications - How ?
- ❖ Resources
- ❖ Q & A

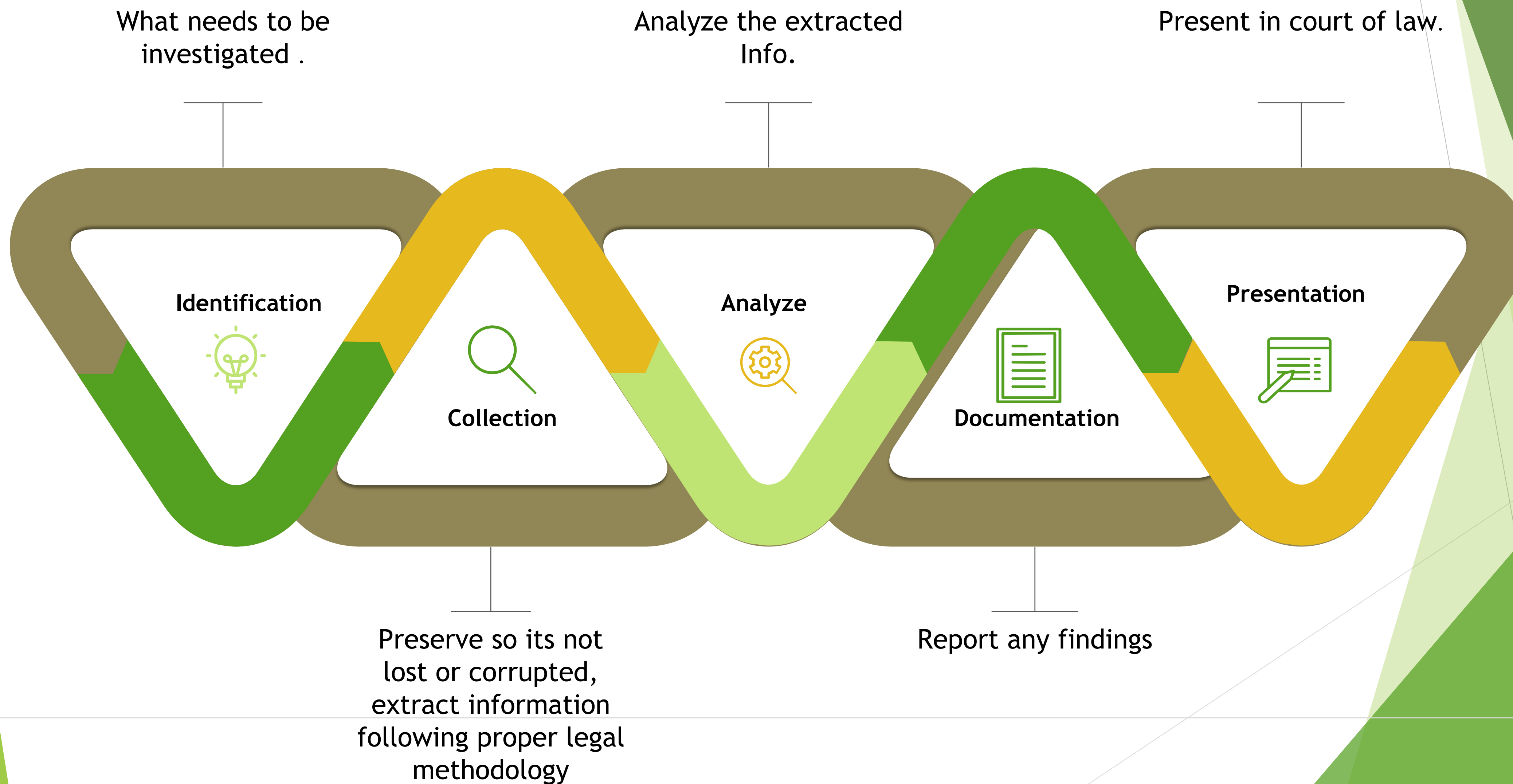


What is Digital Forensics

- ▶ Growth of computers and computer hack started in 1980
- ▶ The Computer Fraud and Abuse Act (1986)
- ▶ The law prohibits accessing a computer without authorization, or in excess of authorization
- ▶ Identify, Preserve, Recover , Analyze and Present the digital evidence from various electronic devices.
- ▶ Devices that works on 0 and 1 : Mobile Phones, PDA's, Smart Watches, Printers, Scanners, Secondary Storage Media, Bio metric Devices.



What is Digital Forensics



The Evolution of Digital Forensics

Year	Who	Evolution
1847 -1915	Hans Gross (Austrian Criminal jurist, Father of criminal profiling)	First use of scientific study to head criminal investigations
1932	FBI	Set up a lab to offer forensics services to all field agents and other law authorities across the USA
1978		The first computer crime was recognized in the Florida Computer Crime Act.
1842-1911	Francis Galton	He devised a method for classifying <u>fingerprints</u> that proved useful in <u>forensic science</u>
1992		The term Computer Forensics was used in academic literature.
1995		International Organization on Computer Evidence (IOCE) was formed.



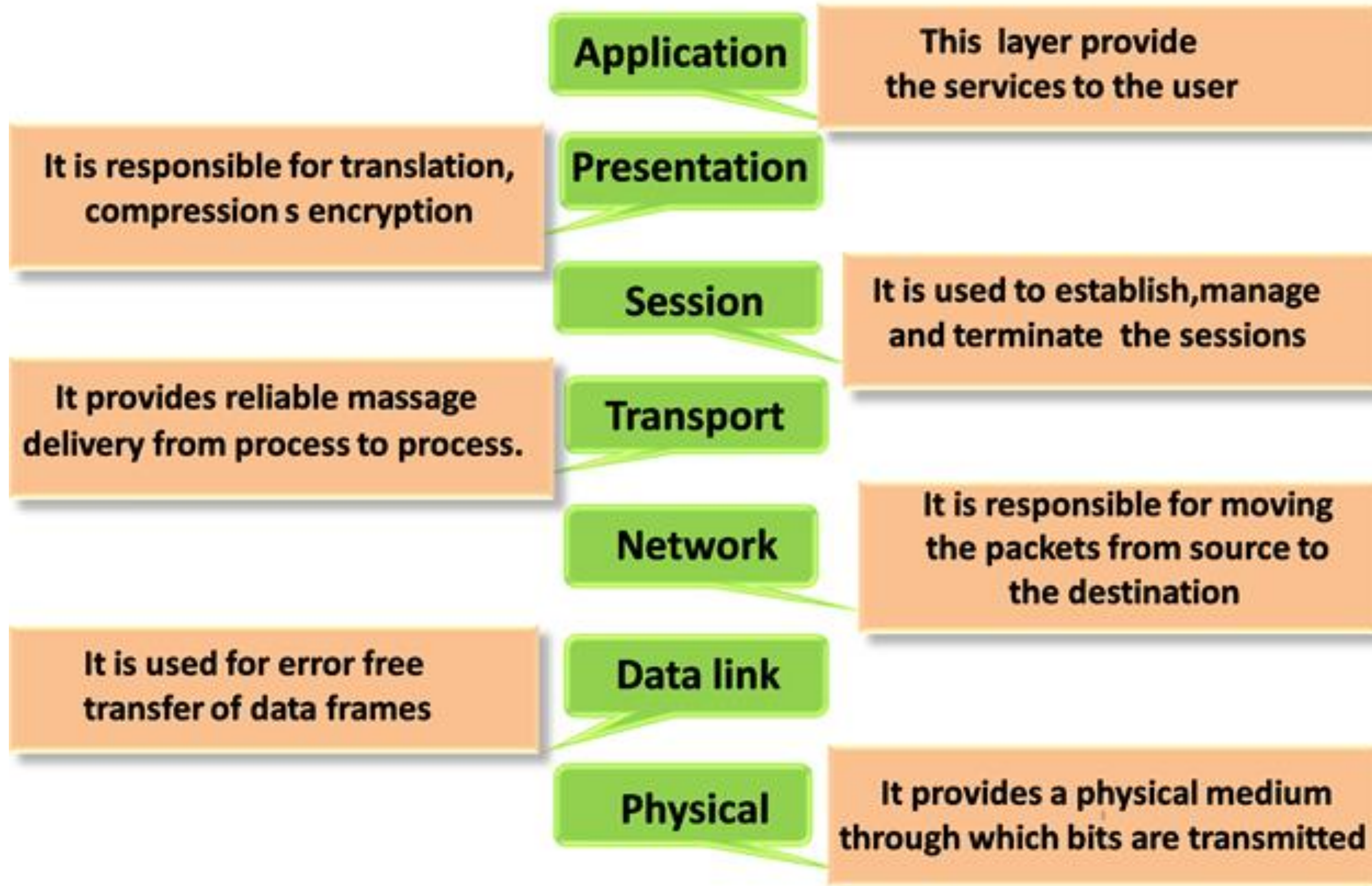
Year	Evolution
1998	EnCase Forensic officially released (originally named Expert Witness for Windows). At the time there were no GUI forensic tools available
2000	First FBI Regional Computer Forensic Laboratory established.
2002	Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called "Best practices for Computer Forensics".
2002	EnCase Enterprise was released allowing the first network enabled digital forensic tool to be used in forensic, investigative
2010	Simson Garfinkel identified issues facing digital investigations.
Past Decade	Evolving with various tools and technologies in the market



Get Started

- ❖ OSI - Layer Model Open System Inter Connection
<https://www.javatpoint.com/osi-model>
- ❖ Forensics Focus - Forensicfocus.com
- ❖ User Groups and Networks
- ❖ <https://www.aisa.org.au/> - Digital Forensic Group
- ❖ Re-Search and go through forensics Tools
- ❖ Get depth of at least one tool
- ❖ Understand the Breadth of the tools
- ❖ Those who are not trained, certified or qualified in the field of digital forensics should refrain from using the word “Forensic” when labeling or describing their reports, work product or when testifying in court.





Java Point :Pic Credit



Skills Required

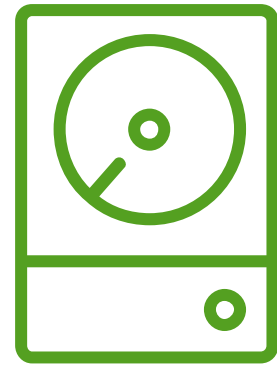
- Networks, Operating System
- Systems or Hardware Would be an advantage
- IT Admin/ InfoSec Professional, next career path opportunity
- Very few skilled people are there in industry
- More than 95% of crime involves digital device in some way
- Degrees of Forensics Critical demand in this field
- Programming Knowledge
- Understand the domain and have passion
- Technical Aptitude , knowledge of digital devices , Analytical Skills
- CyberLaw and Investigation Integrity preserving evidence is important
- No bias, Maintain Investigation credibility as confidential for the case , disciplinary actions



Benefits

- ❖ To present as evidence in a court of law.
- ❖ To determine that the digital evidence obtained is true and honest, track the suspect
- ❖ Examine data and devices to find out max possible breach or crime that involved digital devices
- ❖ The motive behind the crime and identity of the main culprit.
- ❖ Recovering deleted files and deleted partitions from digital media to extract the evidence for validation purpose.
- ❖ Allows to estimate the potential impact of the malicious activity on the victim. Forensic report which offers a complete report on the investigation process.

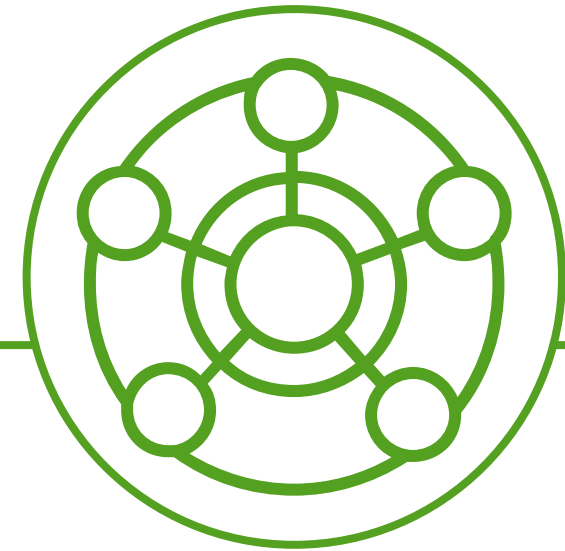
Types



Disk Forensics

extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc..

- Identify digital evidence
- Seize & Acquire the evidence
- Authenticate the evidence
- Preserve the evidence
- Analyze the evidence
- Report the findings
- Documenting



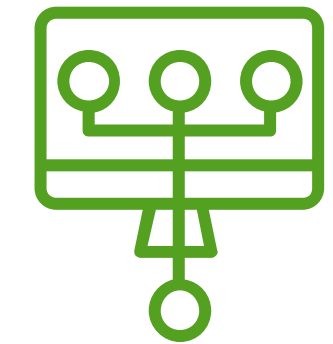
Network Forensics

the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents for intrusion detection and logging



WireLess Forensics

all data moving over the network and analyzing network events to uncover network anomalies, discover the source of security attacks, and investigate breaches on computers and wireless networks to determine whether they are or have been used for illegal or unauthorized activities

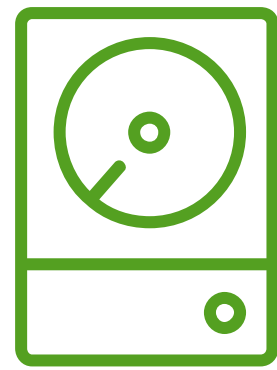


Database Forensics.

The discipline is similar to computer forensics, following the normal forensic process and applying investigative techniques to database contents and metadata **forensics**, following the normal forensic process and applying investigative techniques



Types



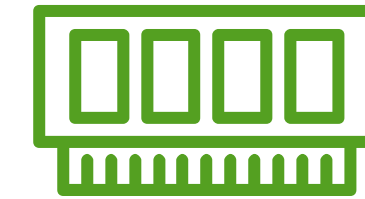
Malware Forensics

the functionality, source and possible impact of a given malware such as a virus, worm, Trojan horse, rootkit



Email Forensics

Email fraud investigation is the collection and forensic investigation of evidence into email hacking, phishing attacks, tracing and recovery of stolen funds. Email Fraud is the intentional deception made for personal gain or to damage another individual through email.



Memory Forensics

analysis of volatile data in a computer's memory dump



MobilePhone

include taped conversations, digital phone pictures, mobile phone texts or emails, phone number lists and sometimes even mobile phone digital video recordings



Types of forensics



OS
of retrieving useful information
from the Operating System (OS)
of the computer or mobile device
in question.



Cloud

Cloud Forensics is actually an
application within Digital Forensics
which oversees the crime
committed over the cloud and
investigates on it



Browser

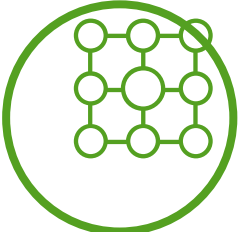


Analysis is a separate,
large area of expertise.
Web browsers are used
in mobile devices,
tablets, netbooks,
desktop



OpenSourceTools

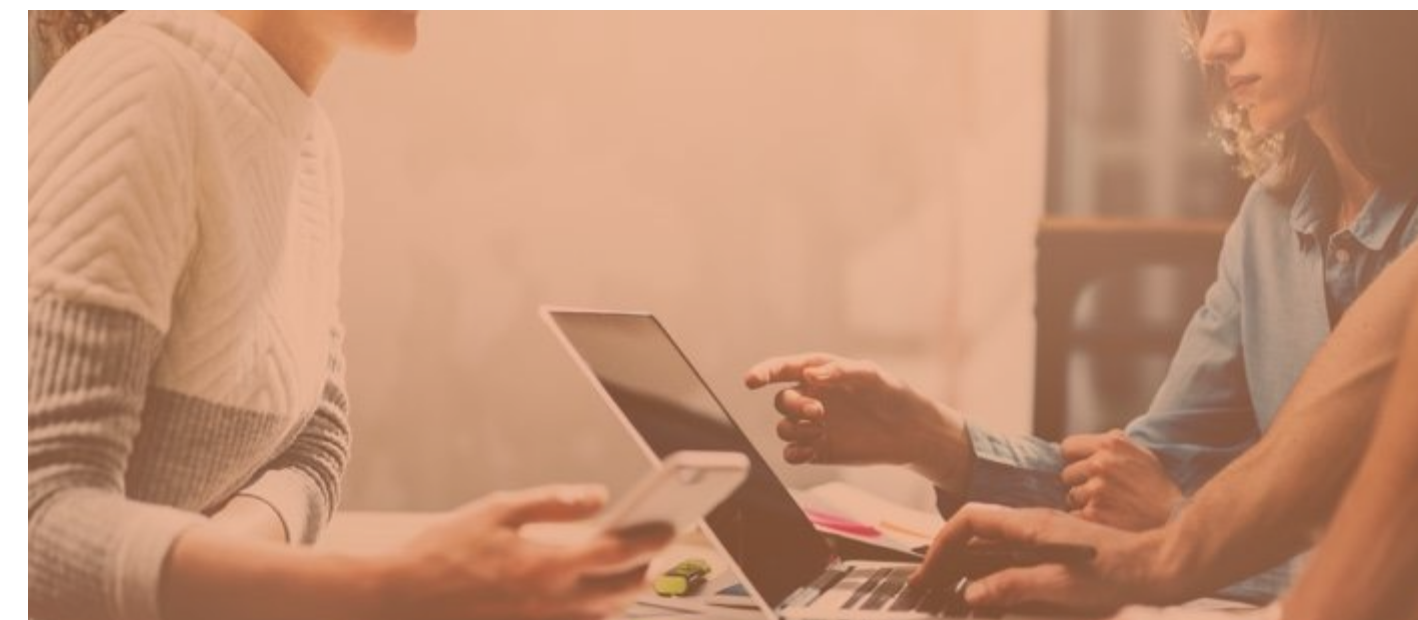
- ❖ Autopsy - fast & efficient hard drive investigation solution
- ❖ Data Dumper - a Command Line Forensic tool to dump segments of data from an original source image or physical/logical device
- ❖ DumpZilla - <https://www.dumpzilla.org/> extracts information from browsers based on Firefox.
- ❖ Ophcrack - <https://ophcrack.sourceforge.io/> for cracking the hashes, Runs on Windows, Linux/Unix, Mac OS X,
- ❖ Volatility - Analyzing RAM in 32 bit/64 bit systems. Supports analysis for Linux, Windows, Mac, and Android systems. Based on Python , can be run on Windows, Linux, and Mac systems

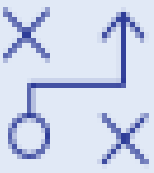
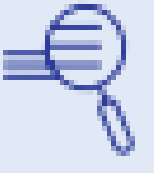



EnCase capabilities

-  MA -AI Visual threat Intelligence
-  Enhanced agent
-  Apple File System (APFS) support
-  Apple T2 Security Bypass
-  Volume shadow copy
-  Easy reporting

"To collect anything for forensic matters, cybersecurity matters or eDiscovery matters or investigations, it's always going to be OpenText EnCase. You know you're doing it right and you know every court is signed off on it. You can go to bed and feel comfortable about that."

Susan Jackson
Legal Counsel
Novelis



-  **Reliable** acquisition of evidence
-  **Deep forensic** analysis
-  **Mobile collection** for 27,000-plus profiles
-  **Image analysis**
-  **Broad OS/ decryption** support
-  **Connect to the cloud**

SC²⁰²⁰ awards
Winner

Certifications

- ❖ CHFI: Computer Hacking Forensic Investigator V9
- ❖ CFCE: Certified Forensic Computer Examiner
- ❖ <https://www.opentext.com/products-and-solutions/services/training-and-learning-services/encase-training/certifications>
- ❖ CCE: Certified Computer Examiner
- ❖ CSFA: Cyber Security Forensic Analyst
- ❖ GCFA (Global Information Assurance Certification) an intermediate-level computer forensics credential that signifies.

<https://www.mosse-institute.com/certifications.html>

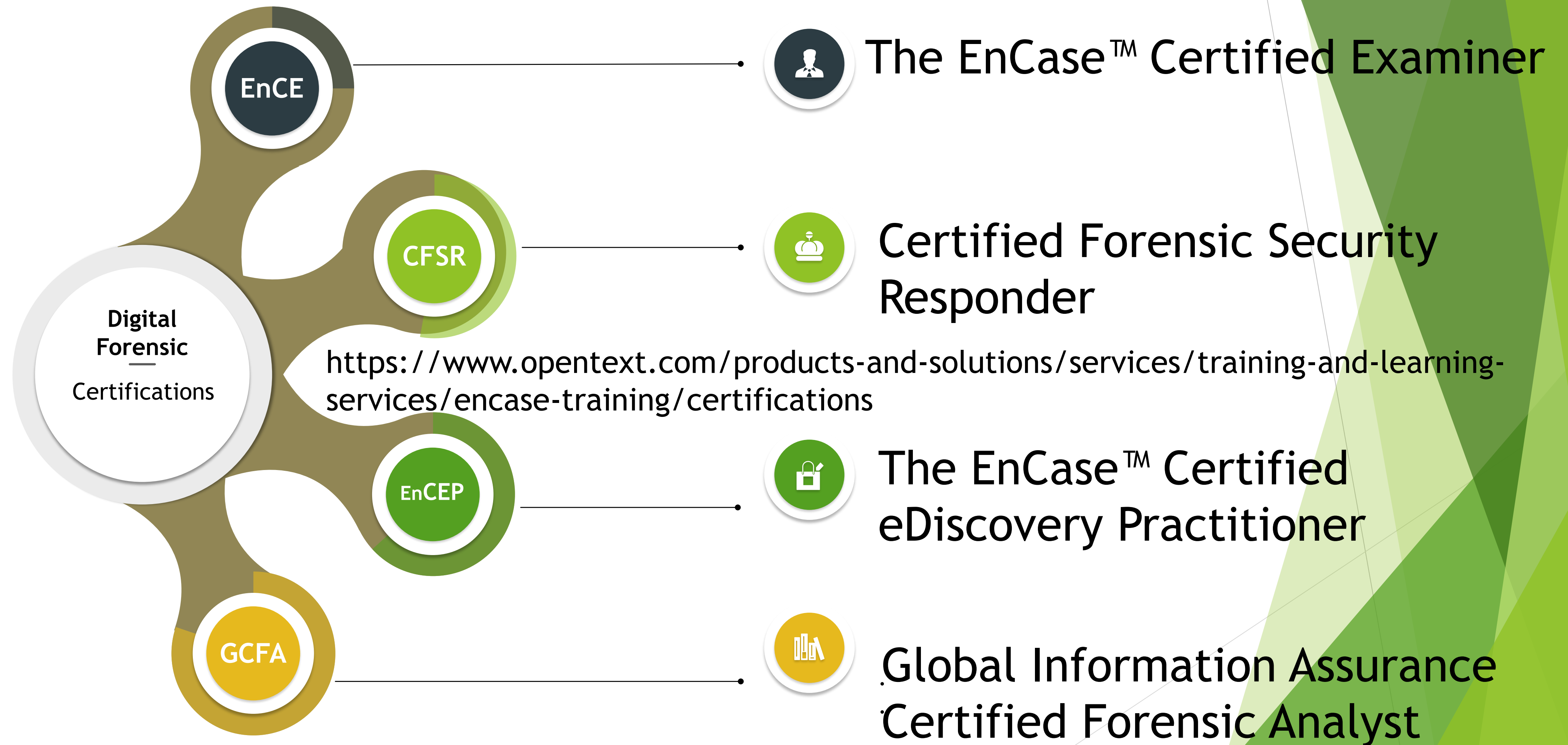
<https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/>

[https://online.champlain.edu/degrees-certificates/bachelors-](https://online.champlain.edu/degrees-certificates/bachelors-computer-forensics-digital-investigations)

[computer-forensics-digital-investigations](https://online.champlain.edu/degrees-certificates/bachelors-computer-forensics-digital-investigations)



Certifications



Use Cases

- ❖ Intellectual Property theft
- ❖ Industrial surveillance
- ❖ Employment disputes
- ❖ Fraud investigations
- ❖ Inappropriate use of the Internet and email in the workplace
- ❖ Forgeries related matters, Criminal Investigations
- ❖ Bankruptcy investigations , Medical Investigations
- ❖ Issues concern with the regulatory compliance
- ❖ Law Enforcement offices , Terroristic attacks
- ❖ Government Agencies
- ❖ Police Department, Defense and Navy many more
- ❖ <https://blog.eccouncil.org/5-cases-solved-using-extensive-digital-forensic-evidence/>



Career Opportunities

[Payscale.com](https://www.payscale.com) (2018) - that people in the field of computer forensics make an average annual salary of \$69,2260 with the top 10 percent of earners bringing home \$110,000.

- ❖ Forensic Computer Analyst
- ❖ Computer Forensics Examiner
- ❖ Security Consultant
- ❖ Mobile Forensics Expert
- ❖ Computer Crime Investigator
- ❖ Cryptanalyst
- ❖ Cryptographer
- ❖ Disaster Recovery Expert
- ❖ Forensic Instructor
- ❖ Trainer
- ❖ Forensic Author or Journalist



Certifications

- ❖ CHFI: Computer Hacking Forensic Investigator V9
- ❖ CFCE: Certified Forensic Computer Examiner
- ❖ CCE: Certified Computer Examiner
- ❖ CSFA: Cyber Security Forensic Analyst
- ❖ GCFA (Global Information Assurance Certification) an intermediate-level computer forensics credential that signifies.

<https://www.mosse-institute.com/certifications.html>

<https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/>

<https://online.champlain.edu/degrees-certificates/bachelors-computer-forensics-digital-investigations>



References

<https://www.guidancesoftware.com/encase-forensic>

<https://eforensicsmag.com/download/learn-how-to-101-best-forensic-tutorials/>

<https://www.mosse-institute.com/>

<https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/>

<https://blog.eccouncil.org/6-skills-required-for-a-career-in-digital-forensics/>

<https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools>

<https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#4def9a3047e8>

<https://blog.eccouncil.org/4-reasons-every-ciso-should-learn-digital-forensics>

<https://www.guru99.com/computer-forensics-tools.html>

<https://blogs.opentext.com/opentext-encase-wins-10th-consecutive-sc-magazine-award-for-best-computer-forensic-solution/>

<https://h11dfs.com/the-best-open-source-digital-forensic-tools/>

<https://resources.infosecinstitute.com/category/computerforensics/introduction/free-open-source-tools/#gref>

<https://en.wikipedia.org/wiki/EnCase>

<https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools>

http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=116&Itemid=49

Summary

- ❖ Digital Forensics is science of preservation, identification, extraction, and documentation of digital evidence which can be used in the court of law
- ❖ Process & Evolution of Digital Forensics
- ❖ Different types of Digital Forensics
- ❖ Tools & Skills Required
- ❖ Digital Forensic Science User Cases & Domains
- ❖ Career opportunities
- ❖ Next Steps



IF THEY DON'T GIVE YOU
A SEAT AT THE TABLE,
BRING A FOLDING CHAIR.

—SHIRLEY CHISHOLM—

Thank you @ForensicHima

<http://linkedin.com/company/CyberPsy>

www.facebook.com/cyberpsyz

Instagram / Twitter : @Cyberpsyz

<https://www.facebook.com/groups/cyberpsy>



GRACE D. CHIN

