Digital Forensics Certification Training for the Department of Homeland Security and State and Local Law Enforcement (FLETC)

Hannah Fell
hannah.fell30@gmail.com

Mentor: Dr. Christie Nelson
christie.l.nelson.phd@gmail.com
“Cyberattacks are the fastest growing crime in the U.S. and they continue to grow in size and sophistication [1].” The increase in these attacks across the nation has made digital forensics an important component of the criminal justice system. Digital forensics is a branch of forensic science involving the recovery and investigation of data from digital devices. This type of evidence can be very useful for providing vital information during investigations. However, it can be challenging for professionals to manipulate, store, access, and use in courtroom settings. To help avoid these challenges, digital forensics professionals should be properly trained and receive relevant certifications.
Overview of CCICADA and REU CINA Project

- Analyze training and certification requirements for digital forensics for Homeland Security investigative units and State and Local Law Enforcement.

- Work with FLETC to identify opportunities and gaps in digital forensics training.

- Recommend digital forensics training and certification pathways to standardize training and certification across all of Homeland Security.
My Project Goals

- Use data science to analyze qualitative and quantitative data:
  - Subject matter of expert interview reports
  - Qualitative input from technical experts, project partners, researchers
  - Ongoing database of available certifications/classes
  - Employment/labor hiring raw data
  - Practitioner survey data
- Interpret and perform data analysis, continually gathering more data as needed
- Gather insights and present findings to practitioners
- Present at professional venue, to practitioners, and make a national impact on training

NOTE: Only a subset of findings will be included in this presentation. Please contact me with any additional questions.
Research Steps and Datasets Analyzed

**Step 1:** Completed Literature Review on the following topics:
- Cybersecurity and digital forensics basics
- Data visualization
- Clustering techniques

**Step 2:** Gather data sets

**Step 3:** Collect questions to be answered by the CINA research team and formulate other interesting questions about the data

**Step 4:** Visualize data in Microsoft Excel

**Step 5:** Interpret results and identify notable discoveries

**Step 6:** Gather insights from the CINA research team

**Step 7:** Repeat analysis from data points and answer any additional questions

**Labor Analysis in Burning Glass,** looked at thousands of relevant job postings/openings and pieces of data over 5–6 years

**Industry Certifications and Courses related to Digital Forensics:** 186 related courses/certifications found by CINA team
**Background Information**

**Cybersecurity**: the practice of protecting systems, networks, and programs from digital attacks [2].

**Digital Forensics**: the practice of identifying, preserving, recovering, analyzing and presenting facts about digital evidence found on computers [3].

**Computer Forensics**: the practice of extracting and preserving data from a computer so that it can be used in a criminal proceeding as evidence [4].

**Cyber Forensics**: the practice of gathering, processing, interpreting, and using digital evidence to provide a conclusive description of cyber crime activities [5].
Certification Analysis Graphic

Certifications
- Number of postings requesting top 25 certifications in each field, 2014-YTD
- Number of postings requesting top 25 specific certifications in each field, 2014-YTD
- Grouping of top 25 certifications based on various categories

Number of postings requesting top 25 certifications in each field by U.S. region, 2014-YTD

Training
- Comparison of courses based on cost, proficiency level, duration, investigation step applicability, forensic category, and delivery method
- Box plot comparison of cost and investigation steps
- Box plot comparison of cost and delivery method
- Box plot comparison of cost and duration
- Box plot comparison of cost, investigation step, and proficiency level
- Box plot comparison of cost, delivery method, and proficiency level
- Box plot comparison of cost, duration, and delivery method

Second Dataset
- Will explain later in presentation
- Box plot comparison of cost, investigation step, and delivery method
Job Opening Analysis
(2014-YTD)

GOAL: Use data science to analyze employment/labor hiring raw data.

Information collected from https://laborinsight.burning-glass.com/jobs/us#/jobs/loginwindow?returnUrl=jobs%2Flicenseagreement

- Data is pulled from corporate website’s job boards and other places where job ads are posted. Ex: Indeed (It scans more than 40,000 sources capturing roughly 85% of all open jobs)
- **NOTE:** Job postings that are missed are typically for small businesses. Ex: Restaurant posting a “Help Wanted” sign in the window. Lower income and lower skilled jobs are less likely to be posted online versus higher skilled jobs. However, online postings have expanded.
The trend lines for computer forensics, digital forensics, and cyber forensics are almost identical. Since the terms are basically interchangeable, this shows which terms employers are using more frequently.

**Greatest to Least:**
1. Cybersecurity
2. Computer Forensics
3. Cyber Forensics
4. Digital Forensics
Why is cybersecurity much greater than any other field, especially from 2016 to YTD?

**Cybersecurity**: Provides protection from cyber attacks **before they happen**. Everyone wants to be protected from cyber breeches, which have been significantly increasing. This means cybersecurity is being used by individuals, businesses, and corporations that have sensitive information. Many companies hire employees that oversee cybersecurity alone [6].

**Digital Forensics**: Investigate and analyze evidence from cyber crimes **after they happen**. Used by any individual, business, or corporation that has experienced a cyber attack that needs further investigation [3].

Typically Digital, Computer, and Cyber Forensics are a subset of Cybersecurity.
Certification Analysis (2014–YTD)

**GOAL:** Use data science to analyze, compare, and identify any opportunities, gaps, or differences between cybersecurity, computer forensics, digital forensics, and cyber forensics certification requirements.


- Data is pulled from corporate website’s job boards and other places where job ads are posted. **Ex:** Indeed (It scans more than 40,000 sources capturing roughly 85% of all open jobs)
- **NOTE:** Job postings that are missed are typically for small businesses. **Ex:** Restaurant posting a “Help Wanted” sign in the window. Lower income and lower skilled jobs are less likely to be posted online versus higher skilled jobs. However, online postings have expanded.
Top 25 Certifications In Demand For Digital Forensics Job Openings Each Year Across U.S.

- CISSP
- SANS/GIAC Security Clearance
- CISM
- GCIA
- GIAC Certified Forensic Analyst
- CISSP
- GIAC Certified Forensic Examiner
- CompTIA Security+
- EnCE
- Information Systems
- CCNA
- CEH
- CompTIA Network+
- Project Management
- SSCP
- GIAC Reverse Engineering Malware Certified Computer Examiner
- MCSE
- GSEC
- Certified A+ Technician
- GIAC Certified Intrusion Analyst
- Driver's License
- PMP
- MCSA
- CFE
- IT Infrastructure Library
- Legacy
- CCNP
- GWAPT
- CCIE
- GIAC Certified Enterprise Defender
- CCFP
- GCIH
- Certified in Risk and Information Systems Control
- GXPN
## Top 10 Certifications From 2014 to YTD

<table>
<thead>
<tr>
<th>Cybersecurity</th>
<th>Computer Forensics</th>
<th>Digital Forensics</th>
<th>Cyber Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security Clearance</td>
<td>1. CISSP</td>
<td>1. SANS/GIAC</td>
<td>1. CISSP</td>
</tr>
<tr>
<td>2. CISSP</td>
<td>2. SANS/GIAC</td>
<td>2. CISSP</td>
<td>2. SANS/GIAC</td>
</tr>
<tr>
<td>4. SANS/GIAC</td>
<td>4. GCIH</td>
<td>4. GCIH</td>
<td>4. GCIH</td>
</tr>
<tr>
<td>5. CISM</td>
<td>5. CISM</td>
<td>5. GIAC Certified Forensic Analyst</td>
<td>5. CISM</td>
</tr>
<tr>
<td>7. IT Infrastructure Library</td>
<td>7. CompTIA Security+</td>
<td>7. GIAC Certified Forensic Examiner</td>
<td>7. CISA</td>
</tr>
<tr>
<td>8. Project Management</td>
<td>8. GIAC Certified Forensic Analyst</td>
<td>8. CISA</td>
<td>8. GIAC Certified Intrusion Analyst</td>
</tr>
</tbody>
</table>
## Similarities/Differences For Certifications (2014–YTD)

<table>
<thead>
<tr>
<th></th>
<th>Cybersecurity</th>
<th>Computer Forensics</th>
<th>Digital Forensics</th>
<th>Cyber Forensics</th>
</tr>
</thead>
</table>
## Groupings of Top 25 Employer Requested Certifications

<table>
<thead>
<tr>
<th>Management</th>
<th>Security/Defense</th>
<th>Background Checks</th>
<th>Network</th>
<th>Computer Software</th>
<th>IT</th>
<th>Investigation</th>
<th>Testing</th>
<th>Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Project Management</td>
<td>● CISSP</td>
<td>● CompTIA Security+</td>
<td>● Drivers License</td>
<td>● CompTIA Network+</td>
<td>● MCSE</td>
<td>● CCNA Information Systems</td>
<td>● ENCE</td>
<td>● CCFP</td>
</tr>
<tr>
<td>● CISM</td>
<td>● SANS/GIAC</td>
<td>● Security Clearance</td>
<td>● CompTIA Network+</td>
<td>● MCSA</td>
<td>● ITIL</td>
<td>● Certified A+ Tech.</td>
<td>● GIAC Certified Forensic Examiner</td>
<td>● CCIE</td>
</tr>
<tr>
<td>● IT Infrastructure Library</td>
<td>● SSCEP</td>
<td>● GSECA</td>
<td>● Java</td>
<td>● CCIE</td>
<td>● CCISC</td>
<td>● CISA</td>
<td>● ABET</td>
<td>● GPEN</td>
</tr>
<tr>
<td>● PMP</td>
<td>● CEH</td>
<td>● GIAC Certified Intrusion Analyst</td>
<td>● MCSE (Legacy)</td>
<td>● CCE</td>
<td>● CCIE</td>
<td>● CISA</td>
<td>● CCSP</td>
<td>● CCNP</td>
</tr>
<tr>
<td>● Master Project Management</td>
<td>● GIAC Certified Intrusion Analyst</td>
<td>● CASP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● GSCL</td>
<td>● GIAC Certified Forensic Analyst GCCH</td>
<td>● GSECA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● GIAC Reverse Engineering Malware</td>
<td>● CFE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● GIAC Certified Enterprise Defender</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Other:** CPA

**NOTE:** Skills in red mean they could fit into multiple categories.
Specialized Skills Analysis
(2014–YTD)

GOAL: Use data science to analyze, compare, and identify any opportunities, gaps, or differences between cybersecurity, computer forensics, digital forensics, and cyber forensics specialized/NIST skill requirements.

Information collected from https://laborinsight.burning-glass.com/jobs/us#/jobs/loginwindow?returnUrl=jobs%2Flicenseagreement

- Data is pulled from corporate website’s job boards and other places where job ads are posted. Ex: Indeed (It scans more than 40,000 sources capturing roughly 85% of all open jobs)
- **NOTE:** Job postings that are missed are typically for small businesses. Ex: Restaurant posting a “Help Wanted” sign in the window. Lower income and lower skilled jobs are less likely to be posted online versus higher skilled jobs. However, online postings have expanded.
<table>
<thead>
<tr>
<th>Cybersecurity</th>
<th>Computer Forensics</th>
<th>Digital Forensics</th>
<th>Cyber Forensics</th>
</tr>
</thead>
</table>
## Similarities/Differences For Skills (2014-YTD)

<table>
<thead>
<tr>
<th>Top 3</th>
<th>Cybersecurity</th>
<th>Computer Forensics</th>
<th>Digital Forensics</th>
<th>Cyber Forensics</th>
</tr>
</thead>
</table>


### Groupings of Top 25 Employer Requested Skills

<table>
<thead>
<tr>
<th>Computer Programming Languages</th>
<th>Soft Skills</th>
<th>Software</th>
<th>Management</th>
<th>Technology</th>
<th>Security/Defense</th>
<th>Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>Scheduling</td>
<td>Software Development</td>
<td>Project Management</td>
<td>Information Systems</td>
<td>Computer Forensics</td>
<td>Litigation</td>
</tr>
<tr>
<td>SQL</td>
<td>Budgeting</td>
<td>Software Engineering</td>
<td>Risk Management</td>
<td>Systems Engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JavaScript</td>
<td>Customer Service</td>
<td>SAP</td>
<td></td>
<td>Linux</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C++</td>
<td>Customer Contact</td>
<td>Splunk</td>
<td></td>
<td>UNIX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Python</td>
<td>Technical Writing/Editing</td>
<td>Empower</td>
<td></td>
<td>Oracle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PERL</td>
<td>Simulation</td>
<td></td>
<td></td>
<td>Information Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft: PowerShell</td>
<td>Business Processes</td>
<td></td>
<td></td>
<td>System Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales</td>
<td></td>
<td></td>
<td>Technical Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Teaching</td>
<td></td>
<td></td>
<td>Computer Engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CISCO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TCP/IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Storage Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Skills in red mean they could fit into multiple categories.
Job Title Analysis (2018)

GOAL: Use data science to analyze, compare, and identify any differences between cybersecurity, computer forensics, digital forensics, and cyber forensics job titles.

Information collected from https://laborinsight.burning-glass.com/jobs/us#/jobs/loginwindow?returnUrl=jobs%2Flicenseagreement

- Data is pulled from corporate website’s job boards and other places where job ads are posted. Ex: Indeed (It scans more than 40,000 sources capturing roughly 85% of all open jobs)
- NOTE: Job postings that are missed are typically for small businesses. Ex: Restaurant posting a “Help Wanted” sign in the window. Lower income and lower skilled jobs are less likely to be posted online versus higher skilled jobs. However, online postings have expanded.
Top 3 Job Titles by U.S. Region

Summary

Number of Postings For The Top 3 Cybersecurity Job Titles by U.S Region in 2018

- Software Development Engineer
- Security Analyst
- Systems Engineer

Job Titles

- Northeast
- Southeast
- Southwest
- Midwest
- West

Number of Postings For The Top 3 Computer Forensics Job Titles by U.S. Region in 2018

- Security Analyst
- Security Engineer
- Information Security Analyst

Job Titles

- Northeast
- Southeast
- Southwest
- Midwest
- West

Number of Postings For The Top 3 Digital Forensics Job Titles by U.S. Region in 2018

- Security Analyst
- Security Engineer
- Cyber Analyst

Job Titles

- Northeast
- Southeast
- Southwest
- Midwest
- West

Number of Postings For The Top 3 Cyber Forensics Job Titles by U.S. Regions in 2018

- Security Analyst
- Cyber Security Engineer
- Security Engineer

Job Titles

- Northeast
- Southeast
- Southwest
- Midwest
- West
### Top 3 Job Titles in 2018

<table>
<thead>
<tr>
<th>Cybersecurity</th>
<th>Computer Forensics</th>
<th>Digital Forensics</th>
<th>Cyber Forensics</th>
</tr>
</thead>
</table>

### Top 10 Job Titles in 2018

<table>
<thead>
<tr>
<th>Cybersecurity</th>
<th>Computer Forensics</th>
<th>Digital Forensics</th>
<th>Cyber Forensics</th>
</tr>
</thead>
</table>
Digital Forensics Training Analysis (YTD)

**GOAL:** Use data science to recommend and standardize training and certification pathways by analyzing the ongoing database of available courses in order to identify any opportunities, gaps, or differences between cybersecurity, computer forensics, digital forensics, and cyber forensics training.

Information collected from the Excel spreadsheet titled, “Digital Forensics Training Database.”
Training

Comparison of courses based on cost, proficiency level, duration, investigation step applicability, forensic category, and delivery method

- Box plot comparison of cost and investigation steps
- Box plot comparison of cost and delivery method
- Box plot comparison of cost and duration
- Box plot comparison of cost, delivery method, and proficiency level
- Box plot comparison of cost, duration, and proficiency level
NOTE: 98 courses and 335 entries were used to create this graph since courses without a cost, courses without at least one of the 8 investigation steps, and courses without a proficiency level were not used. Also, for courses that had a price range rather than an exact price, the start and end values of the range were used. Ex: If the price range for a course was $1,000-$2,500, then $1,000 and 2,500 were used.
INTELLIGENCE IS THE MOST EXPENSIVE STEP

NOTE: 103 courses and 342 entries were used to create this graph since courses without a cost and courses without at least one of the 8 investigation steps were not used. Also, for courses that had a price range rather than an exact price, the start and end values of the range were used. Ex: If the price range for a course was $1,000-$2,500, then $1,000 and 2,500 were used.
NOTE: 117 courses and 179 entries were used to create this graph since courses without a cost and courses without at least one of the 8 investigation steps were not used. Also, for courses that had a price range rather than an exact price, the start and end values of the range were used. Ex: If the price range for a course was $1,000-$2,500, then $1,000 and 2,500 were used.
9-15 DAY COURSES ARE THE MOST EXPENSIVE

NOTE: 66 courses and 70 entries were used to create this graph since courses without a cost and courses without a duration were not used. Also, each duration option for every class was used. Also, for courses that had a price range rather than an exact price, the start and end values of the range were used. Ex: If the price range for a course was $1,000-$2,500, then $1,000 and 2,500 were used.
There are more courses that last 1 to 4 days and 5 days than 6 days and 7 or more put together.
What’s Next?

More Research and Analysis:

- Analyze the # of job postings for the top 3 job titles by requested skills and certifications.

- Complete year to year trend analysis of job titles for the last 5 years by popularity and title similarities. Then determine which titles are part of the public sector (policing, government, homeland security, secret service, dept of defense, etc) and do trend analysis of them as well.

- Analyze course outlines and use a software program to cluster any commonalities between them. Also, determine if the courses cover NIST Special Publications, NIST Security Standards, or NIST Cybersecurity Framework
Conclusion

This is an ongoing project, but I hope the research I have done and continue to do will contribute to the CINA project team’s research regarding the certification and training requirements for the Department of Homeland Security and State and Local Law enforcement for the Federal Law Enforcement Training Center (FLETC).
Thank you to my mentor, Dr. Christie Nelson, the DIA grant provided by the Rutgers Intelligence Community Centers for Academic Excellence–Critical Technology Studies Program, and the following:

- DIMACS REU (reu.dimacs.rutgers.edu)
- CCICADA (ccicada.org)
- CINA project team
- FLETC (fletc.gov)
- MBS Externship Exchange program (mbs.rutgers.edu/externshipsh)
References


