What do incident response practitioners need to know? A skillmap for the years ahead

By:
Radek Hranicky (Brno University of Technology), Frank Breitinger (University of Liechtenstein), Ondrej Rysavy (Brno University of Technology), John Sheppard (Waterford Institute of Technology), Florin Schaedler (University of Liechtenstein), Holger Morgenstern (Albstadt-Sigmaringen University) and Simon Malik (Albstadt-Sigmaringen University)

From the proceedings of
The Digital Forensic Research Conference
DFRWS USA 2021
July 12-15, 2021

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

https://dfrws.org
What do incident response practitioners need to know?

A skillmap for the years ahead

Radek Hranický
Ondřej Ryšavý
Florin Schaedler
Simon Malik
Frank Breitinger
John Sheppard
Holger Morgenstern
Call for Experts

- Growing need for Digital Forensics and Incident Response (DFIR) professionals
  - Law enforcement
  - Private sector
- Big jump in cybersecurity job postings
  - 74% from 2007 to 2013, double the rate of all other IT jobs\(^1\)
  - 97% from 2013 to 2019, 13% of all IT jobs\(^2\)
- Shortage of trained specialists worldwide

\(^1\) (Vincze, 2016)
\(^2\) (Zan & di Franco, 2020)
Official Statements

**USA:** "82% of employers report a shortage of cybersecurity skills, and 71% believe this talent gap causes direct and measurable damage to their organizations." (J. A. Lewis, US CSIS 2019)

**UK:** "The challenge is much more complex than simply a shortage of cybersecurity professionals – there is a broader cybersecurity capability gap in the UK." (HM Government, 2018)

**France:** "The content and number of initial training and higher education programmes for cybersecurity professions do not meet the needs of businesses and administrations." (Premier Ministre, 2015)

**Germany:** "The shortage of IT security specialists no longer affects only the economy, but also increasingly the public sector." (Schuetze, 2018)

**Italy:** "Italy has a vast problem in relation to cybersecurity education." (Presidenza del Consiglio dei Ministri, 2018)
Issues

"Training is a serious problem facing organizations that deliver forensic services. As a result, many organizations report that it typically takes between one and two years of on-the-job training before a newly minted forensics examiner is proficient enough to lead an investigation." (Garfinkel, 2000)

• Several studies\(^1\) identified a major issue in the lack of:
  • Adequate skills & training
  • Certifications, standards and guidelines

• Others\(^2\) revealed:
  • Limited offering of cybersecurity courses in computer science curricula
  • Poor alignment between education offering and labor market demands
  • Mostly theory-based, insufficient focus on practical exercises

\(^1\)(Henry et al., 2013; Ruefle et al., 2014; Vincze, 2016; Harichandran et al., 2016; Forensic Focus survey 2016 & 2018, Stamaugh, 2000; Garfinkel, 2000)
\(^2\)(Vishik & Heisel, 2015; Zan & di Franco, 2020)
Our Roadmap

1. **Identify the essential DFIR skills based on:**
   - Expert survey: "What do experts think is needed?"
   - Analysis of existing training courses: "What is currently being taught?"
   - Analysis of job listings: "What the market demands?"

2. **Create a map of these skills to:**
   - Answer what skill domains are the most crucial
   - Provide tips for creating new training courses & adjusting existing ones

3. **Develop a "pilot" training course (in progress)**
   - Theoretical part
   - Hands-on labs

4. **Share it with the public and make a "test run" (planned for 2022/2023)**
   - a semester course or 1-week intense seminar

https://sites.google.com/vutbr.cz/dfir-alliance
Survey of DFIR Practitioners

- 15 questions (Open-ended, Multi-choice, Y/N)
- Survey was sent to 40 practitioners from countries around the EU:
  - Germany, Austria, Ireland, Netherlands, Czech Republic, Liechtenstein, ...
- 32 respondents:
  - 34% - Law enforcement / Government agencies
  - 66% - Private sector (Hi-tech, Forensics consulting, Engineering, Financial, Health Care, Logistics, Manufacturing, Retail, ...)

How large is your organization in terms of employee number?

- 72.7%: 1-10 employees
- 18.2%: 11-50 employees
- 51-100 employees
- 101-500 employees
- >500 employees

How many years of experience do you have in DFIR (or a closely related field)?

- 30.3%: less than 2 years
- 36.4%: 2-5 years
- 27.3%: 6-10 years
- 16.0%: more than 10 years
Survey of DFIR Practitioners

How did you get your experience/knowledge and how you stay up to date? [OE]

- 50% - academic qualification in fields related to cybersecurity / forensics
- 88% - non-academic training
  - 53% - Vendor-neutral training by SANS, etc.
  - 19% - Vendor-specific training
  - 16% - In-house training & discussion with colleagues
- 63% - self-learning from conference & journal papers
- 22% - learning on the job
- 16% - capture-the-flag competitions, hackatons, etc.
- 16% - community interaction
Survey of DFIR Practitioners

Which 5 skills are the most essential on a daily basis? [OE]

- Hard skills
  - 44% - Knowledge of software & scripting
  - 40% - Knowledge of computer networks
  - 21% - Ability to use general forensics tools
  - ...

- Soft skills
  - 31% - communication (written & verbal)
  - 13% - critical thinking
  - 13% - attention to detail
  - ...

Survey of DFIR Practitioners

**What tools and technologies do you primarily use? [OE]**

- 99 different tools identified
- The TOP were:
  - 19% - Autopsy
  - 16% - EnCase
  - 16% - Linux utilities
  - 16% - Self-built tools & scripts
  - 9% - Splunk, Wireshark, Volatility framework
- Other repeated answers:
  - AccessData FTK Imager, Moloch, X-Ways, EDRs, Ghidra, IDA, KAPE/Zimmerman, Magnet, MISP, NetworkMiner, NUIX, Renmux, SIFT, Zeek, ...
Survey of DFIR Practitioners

What are the primary challenges you face in your investigations? [OE]

- Encrypted data: 58%
- Insufficient resources: 42%
- Cloud computing: 39%
- Big data problem: 23%
- Legislation: 19%
- Lack of adequate tools: 10%

Challenges appearing in 10%+ responses
Analysis of DFIR Courses

Methodology

1. Collection
   • Keyword-based search: "DFIR, Digital Forensics, Incident Response, Course, Training, Education, …"
   • 42 courses

2. Initial assessment
   • Filtered to results that: a) were legitimate, b) provided sufficient level of detail to extract information
   • Reduced to 37 courses (17 academic; 20 private sector: SANS, IACIS, Udemy, …)

3. Manual analysis
   • Review of courses (topics, description, curricula, …)
   • Identification of most frequently taught skills
Analysis of DFIR Courses

Findings

• Only few courses explicitly advertise themselves as Incident Response
• Majority were part of broader education programs
• Academia
  • Focus on DFIR is more frequent in MSc programs then BSc
  • Most programs (BSc, MSc) do not have a dedicated course on IR but incorporate it into other classes
  • Many universities at least offer 1-2 courses related to DF
• Private sector
  • Majority require fundamental knowledge from computer science & security
  • These prerequisites have to be acquired beforehand
  • Typical duration: 2 to 6 days of training
Analysis of DFIR Courses

Skills

• Most frequent
  • 73% - Investigation Techniques (DF process, methodology, …)
  • 65% - Network Forensics (traffic capturing, protocols, device analysis)
  • 57% - OS Forensics (mobile devices, Windows, Linux, Mac OS X)
  • 57% - Data Acquisition

• Other findings
  • Legal issues (22%), Ethical aspects (19%), Standards (3%) were often not part of the courses
  • Newer topics like IoT Forensics (5%) & Cloud Forensics (3%) were seen very rarely
Job Listings Review

Methodology

1. Selection
   - Keyword-based search on LinkedIn from January 25\textsuperscript{th} to 31\textsuperscript{st} 2021
   - Initial search revealed from 200 to 22,000 jobs worldwide (depending on keywords used)
   - Downloaded several listings per region (EU states, Switzerland, USA)
   - Deleted non-English listings

2. Collection
   - Data set: JobID, date, company name, industry, location, description, required skills, required qualification
   - Removed listings that were too general or not related to DFIR domain
   - Resulting in 66 job listings

3. Analysis:
   - Manual examination of listings
   - Evaluation of required skills
Job Listings Review

Findings

- Most jobs in major cities, some offered remote work
- Many from well-known tech organizations like Facebook, CrowdStrike, Amazon, …
- Education requirements
  - 48% - at least BCs degree in computer science; 5% MSc; 3% PhD
  - 44% - did not mention specific requirements (especially bigger corporations)
  - 15% - required certification from GIAC, CISSP, etc.
  - Many state equivalent practical experience is equally valued
- Most asked for experience
  - Even for entry-level positions
  - Offers for internships are generally very low
Job Listings Review

• Mostly required hard skills
  • Incident Handling (79%)
  • Data Analysis (42%)
  • Security Event & Incident Logging (39%)
  • Network Forensics (38%)
  • Data Acquisition (18%)

• Majority required proficiency general-purpose scripting languages
  • Python, PowerShell, Ruby, Perl, Bash, …

• Soft skills required
  • Mostly overlapping: Analytic & logical thinking, being a team player, flexibility, discretion, …
  • Strong interest in DFIR or related fields
  • Proficiency in English (written & spoken)
DFIR Skillmap

Methodology

1. Classification of skills
   - Tree\(^1\) of 132 skills in four levels (L1 to L4) with DFIR as root (L1)
   - Second level (L2) has 14 skills, inspired my the ACM Computing Classification System\(^2\)
   - Other sources: scientific papers, courses, teaching programs, websites, blogs, ...

2. Creation of the skill matrix
   - Each row represents a skill
   - Each column stands for a data record (R\(_1\), R\(_2\), …)
   - 32 survey answers, 37 courses, 66 job listings
   - "X" is a match
   - Match for a skill triggers a match for the upper-level skill in the same column

3. Assessment
   - For each skill, we calculated the percentage of matches in: survey answers, courses, job listings
   - **Average match ratio** used to estimate each skill’s overall importance

---

\(^1\) Complete tree available at: [https://sites.google.com/vutbr.cz/dfir-alliance/documents](https://sites.google.com/vutbr.cz/dfir-alliance/documents)

\(^2\) See [https://dl.acm.org/ccs](https://dl.acm.org/ccs)
Results

The ranking of L2 skills:

Complete skillmap available at: https://sites.google.com/vutbr.cz/dfir-alliance/documents
Network Forensics

- Encrypted traffic analysis - big challenge, rarely covered by courses
- Security event & incident logging - high demand, poor offering in courses

Top L3 skills in Network Forensics
Incident Handling

- Frequently mentioned in both job listings & survey answers
  - Job listings are more concrete
  - Survey provides very little information about what particular L3 skills are needed most
- Area seems to be fairly covered by existing courses

Top L3 skills in Incident Handling
System Forensics

• Windows Forensics is the most wanted (70% of desktop market share)
• Linux Forensics are the 2nd (major OS on servers)
• What's about Mobile Forensics?
  • Existing courses cover this area more than other systems
  • 0% demand in job listings
  • Is the importance of this area overrated?

Top L3 skills in System Forensics
Conclusion

• Much of existing courses' content is still relevant, but there are gaps to be filled
• Significant difference between professionals' opinions on required skills and the contents of courses, e.g. analysis of encrypted data
• Most employers want previous work experience in the domain
• Importance of hand-on training
• Soft skills were also frequently mentioned and are equally important