2021 SANS Digital Forensics Survey

Digital Forensic Essentials and Why Foundations Matter

Today's Speaker

Jason Jordaan

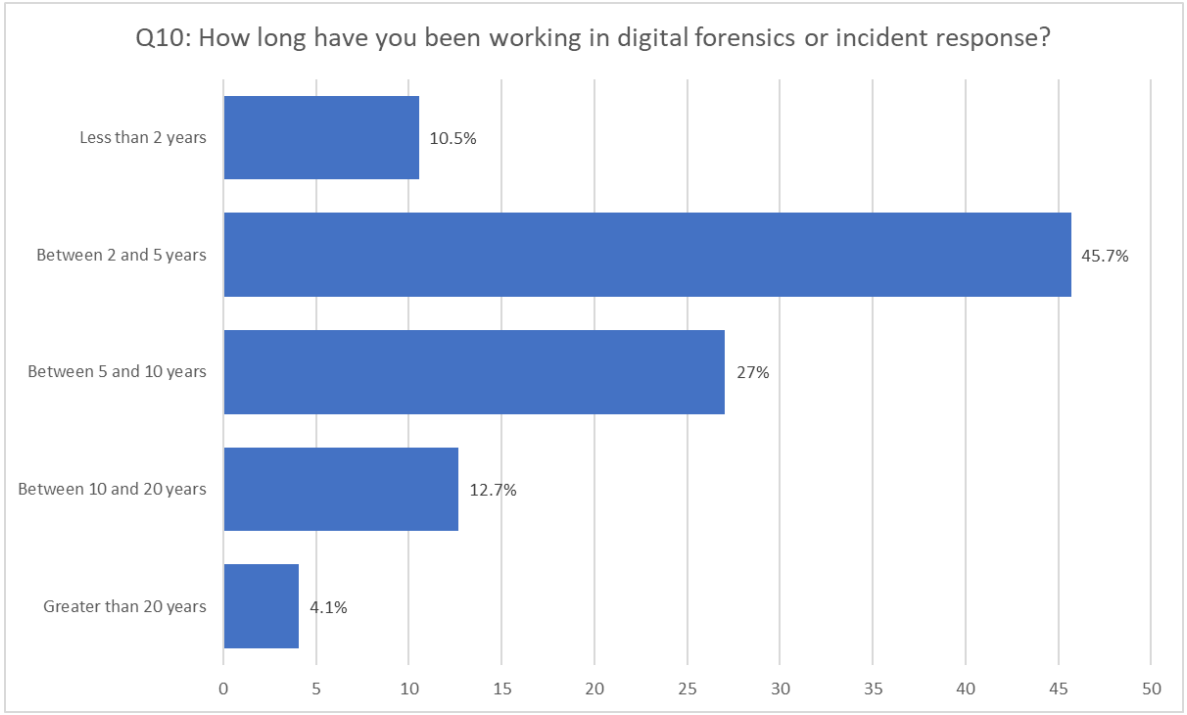
Certified SANS Instructor
FOR308, FOR500, and FOR508
Co-Author FOR308

@DFS_JasonJ

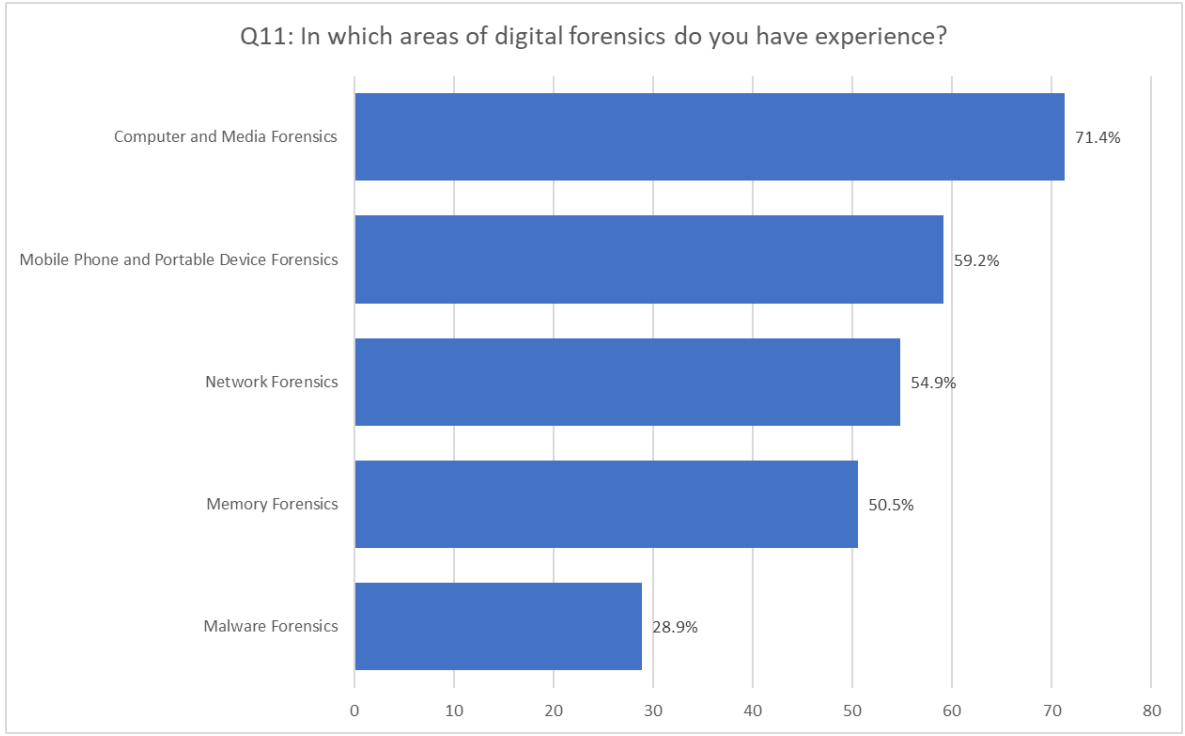
Today's Agenda

- Respondents' Profile
- Digital Forensics Foundation Model
- Core Disciplines
- Foundation Knowledge, Understanding and Skills
- Essential Knowledge, Understanding and Skills
- Consequences of Poor Digital Forensics
- Findings
- Recommendations

Experience in Digital Forensics

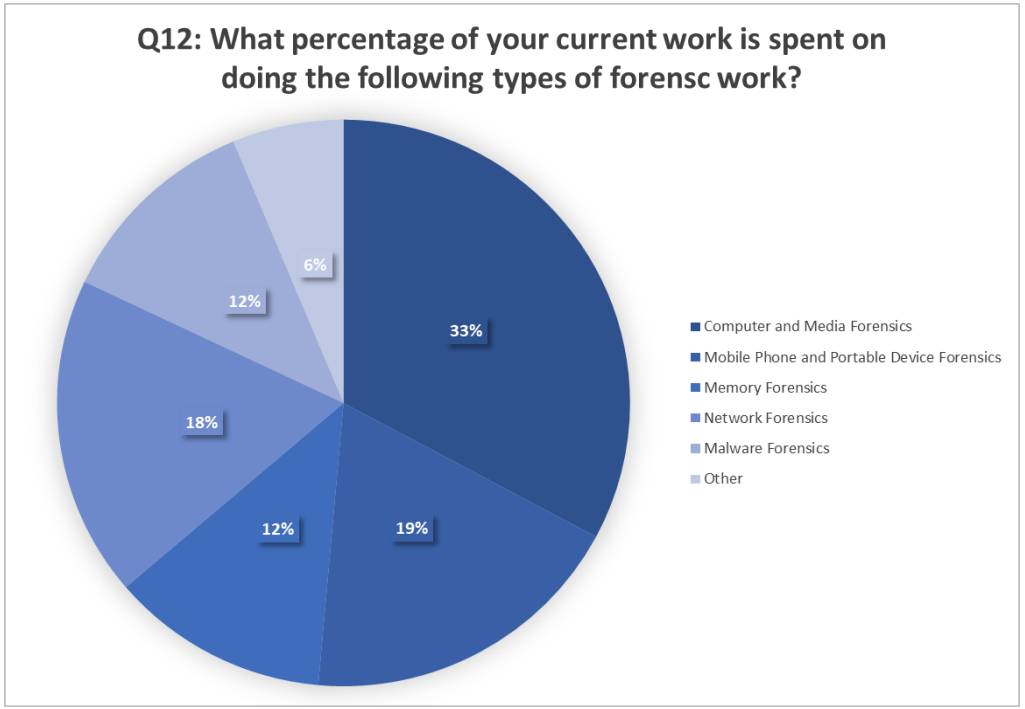


Areas of Experience

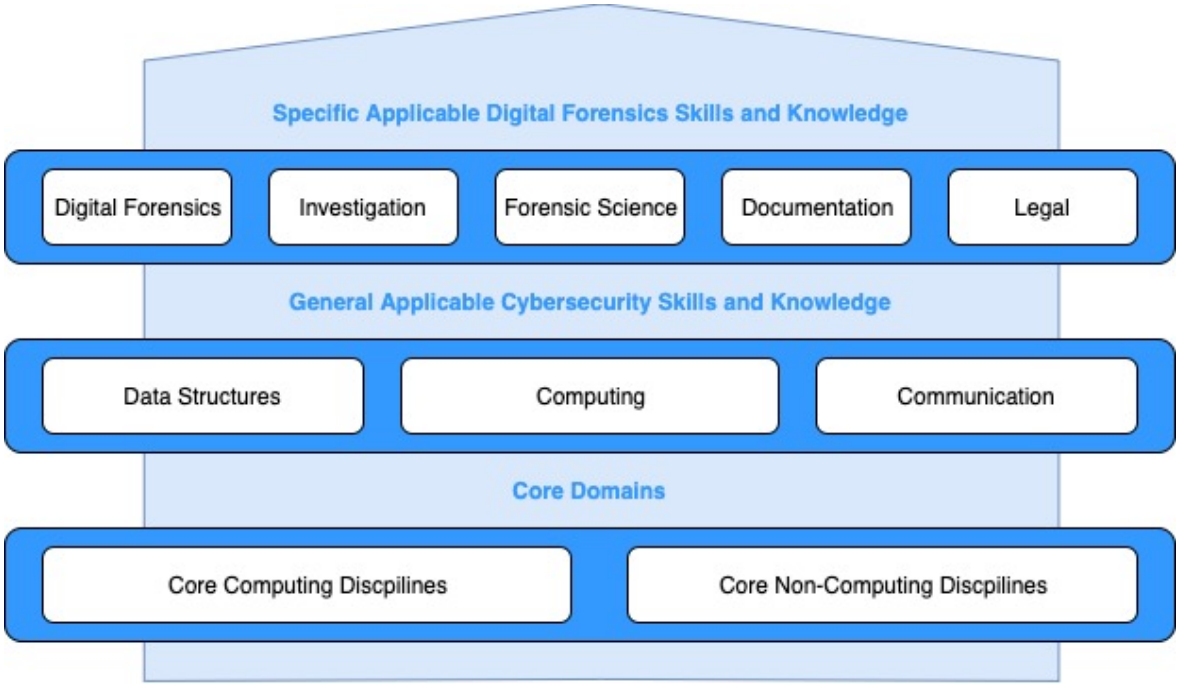


Current Average Digital Forensics Work Breakdown

Analyst Program



Digital Forensics Foundation Model



Overall Importance of Core Computing Disciplines

Analyst Program

How Important are the Following Computing Disciplines in the Practice of Digital Forensics				
Discipline	Overall Importance	Critical	Important	Not Important
Computer Science (primarily systems, software methodology, and application technology)	92.5%	37.6%	54.9%	7.6%
Software Engineering (primarily the design, implementation, and maintenance of software systems)	88.7%	29.5%	59.2%	11.4%
Computer Engineering (primarily hardware, architecture and system orientated)	84.6%	31.4%	63.2%	5.4%

Importance of Non-Computing Core Disciplines

Analyst Program

How Important are the Following Domains in the Practice of Digital Forensics				
Discipline	Overall Importance	Critical	Important	Not Important
Communications	92.4%	42.4%	50%	7.6%
Data Analysis	92.2%	46.2%	46%	7.8%
Investigation	90.8%	46.2%	44.6%	9.2%
Ethics	89.2%	39.5%	49.7%	10.8%
Law and Legal Issues	88.9%	30.5%	58.4%	11.1%
Mathematics and Statistics	88.7%	26.8%	61.9%	11.4%
Criminology	86%	25.7%	60.3%	14.6%
Forensic Science	85.4%	35.4%	50%	14.6%

Importance of Foundation Knowledge and Understanding of Data Structures

Analyst Program

How Important do you Consider the Following Skills and Knowledge as Foundations for the Practice of Digital Forensics and Incident Response				
Discipline	Overall Importance	Critical	Important	Not Important
Interpreting files and data structures at both a hexadecimal and binary level	93.3%	34.6%	58.7%	6.8%
Understanding different time formats	90.5%	39.7%	50.8%	9.5%
Understanding metadata	90.3%	44.1%	46.2%	9.8%
Understanding different data formats	89.2%	33.2%	56%	10.8%
Knowing the difference between little endian and big endian, and why it matters	89.2%	30%	59.2%	10.9%
Understanding file signatures and file headers	88.2%	41.4%	46.8%	11.9%
Understanding file permissions	86.5%	40%	46.5%	13.5%
Recognizing and being able to work with common data encoding types	86.5%	28.7%	57.8%	13.5%
Understanding binary operations	83.7%	33.2%	50.5%	16.2%

Importance of Foundation Computing Knowledge and Skills

Analyst Program

How Important do you Consider the Following Skills and Knowledge as Foundations for the Practice of Digital Forensics and Incident Response				
Discipline	Overall Importance	Critical	Important	Not Important
Understanding how one-way hashing works	90.5%	36.2%	54.3%	9.5%
Understanding how data storage mediums work	89.2%	35.4%	53.8%	10.9%
Understanding how operating systems work from a user perspective	88.9%	40.8%	48.1%	11.1%
Understanding file systems	88.2%	42.2%	46%	11.9%
Understanding computing performance considerations	86.8%	30.8%	56%	13.2%
Skill in navigating data structures in hexadecimal	84.9%	31.9%	53%	15.1%
Skill in using hex editors	84.4%	30.3%	54.1%	15.7%
Skill in the use of command line terminals and instructions	84.3%	35.1%	49.2%	15.7%
Skill in the use of scripting languages	83.6%	27.6%	56%	16.5%

Importance of Foundation Communication Skills

Analyst Program

How Important do you Consider the Following Skills and Knowledge as Foundations for the Practice of Digital Forensics and Incident Response				
Discipline	Overall Importance	Critical	Important	Not Important
Skill in effectively communicating in writing	88.9%	40.5%	48.4%	11.1%

Importance of Essential Digital Forensics Skills and Knowledge

Analyst Program

How Important are the Following Essentials for your Practice of Digital Forensics and Incident Response				
Discipline	Overall Importance	Critical	Important	Not Important
How to conduct effective string searches across data sets	96.3%	38.7%	57.6%	3.8%
Knowing and implementing the digital forensics process	93.8%	44.6%	49.2%	6.2%
Knowing where your tools get their data from	91.9%	41.1%	50.8%	8.1%
Understand forensic acquisition principles	88.9%	42.4%	46.5%	11.1%
Understanding forensic examination and analysis principles	89.5%	43.5%	46%	10.5%
Understanding the digital forensic principles	88.1%	43.5%	44.6%	11.9%
Knowing and implementing the incident response process	87.3%	41.9%	45.4%	12.7%

Importance of Essential Investigation Skills and Knowledge

Analyst Program

How Important are the Following Essentials for your Practice of Digital Forensics and Incident Response				
Discipline	Overall Importance	Critical	Important	Not Important
Identifying different type of investigative environments in which digital forensics is used	91.1%	39.5%	51.6%	8.9%
Applying critical thinking in a case	90.9%	41.4%	49.5%	9.2%
Planning and building an investigation	88.7%	35.7%	53%	11.4%
Applying indictive and deductive reasoning in an investigation	88.4%	34.9%	53.5%	11.6%

Importance of Essential Forensic Science Skills and Knowledge

Analyst Program

How Important are the Following Essentials for your Practice of Digital Forensics and Incident Response				
Discipline	Overall Importance	Critical	Important	Not Important
Understanding and applying the Locard Principle	97.5%	45.1%	52.4%	2.4%
Understanding and applying the Inman-Rudin Paradigm	96.5%	43%	53.5%	3.5%
Understanding and implementing the SWGDE standards	94.2%	37.6%	56%	6.5%
Applying the scientific method during the analysis of evidence	88.6%	36.2%	52.4%	11.4%
The application of quality assurance practices in digital forensics	86.2%	30.5%	56.2%	13.2%
Understanding and implementing the ISO digital forensics and incident response guidelines	86%	27.3%	58.7%	14.1%

Importance of Essential Documentation Skills and Knowledge

Analyst Program

How Important are the Following Essentials for your Practice of Digital Forensics and Incident Response				
Discipline	Overall Importance	Critical	Important	Not Important
Writing forensic reports	91.1%	44.1%	47%	8.9%
How to document and maintain chain of custody	73.5%	33.5%	40%	26.5%
How to make contemporaneous notes and maintain the integrity thereof	91.7%	38.7%	53%	8.4%

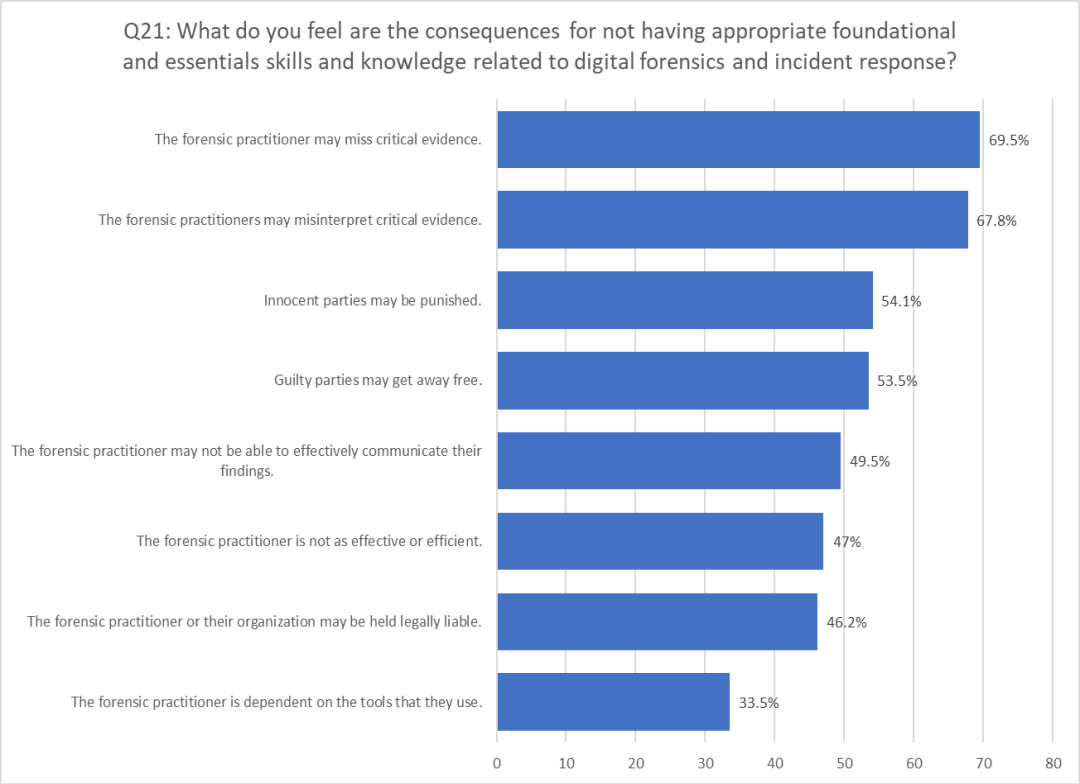
Importance of Essential Legal Skills and Knowledge

Analyst Program

How Important are the Following Essentials for your Practice of Digital Forensics and Incident Response				
Discipline	Overall Importance	Critical	Important	Not Important
Testifying in court	84.3%	26.2%	58.1%	15.7%
Understanding legal elements of matters being investigated	87.6%	33.8%	53.8%	12.4%
Legal processes to secure digital evidence	82.9%	29.7%	53.2%	17%
How to ensure legal authorization for digital forensics	76%	29.2%	46.8%	24%

The Consequences of Poor Digital Forensics Foundations

Analyst Program



Key Findings

- Most respondents confirmed the importance of the core, foundation and essentials for digital forensics.
- Several respondents did not consider these important, which is a concern, indicating potential shortcomings in training and/or education, both initial and ongoing.
- Respondents identified the consequences of poor digital forensics, which could become material as a result of several of the core, foundation and essentials, being considered not important.

Recommendations

- We need to ensure that our competency assessment of digital forensic examiners includes the core, foundation and essentials.
- Training and education of digital forensic practitioners should include the core, foundation and essentials.
- Ongoing continuing professional education should include the core, foundation and essentials.

Acknowledgments

Thanks to all the respondents for participating in the survey.

And to our attendees, thank you for joining us today!

The research paper will be available at https://www.sans.org/white-papers/ the week of July 26, 2021.