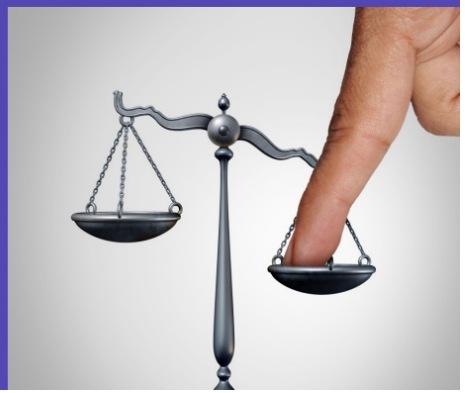

Strengthening Trust in DFIR
We are stronger together!
Diminished Trust
21st Century Skills
Revamping Scientific Practices
Knowledge is Powerful but...
Empowering Equity
SANS DFIR SUMMIT 2020
Eoghan Casey & Daryl Pfeif

Diverse Problems

CSAM, ransomware, data breach, ICS attacks, financial fraud, surveillance, online scams & card skimming...

Need to bolster DFIR...



Developing Diversity in DFIR

Educate more people to fill the gap.
Expand community engagement.
Bring more diverse perspectives.

CRITICAL THINKING & PROBLEM SOLVING
Evidence-based reasoning & evaluating alternatives

Stronger DFIR workforce

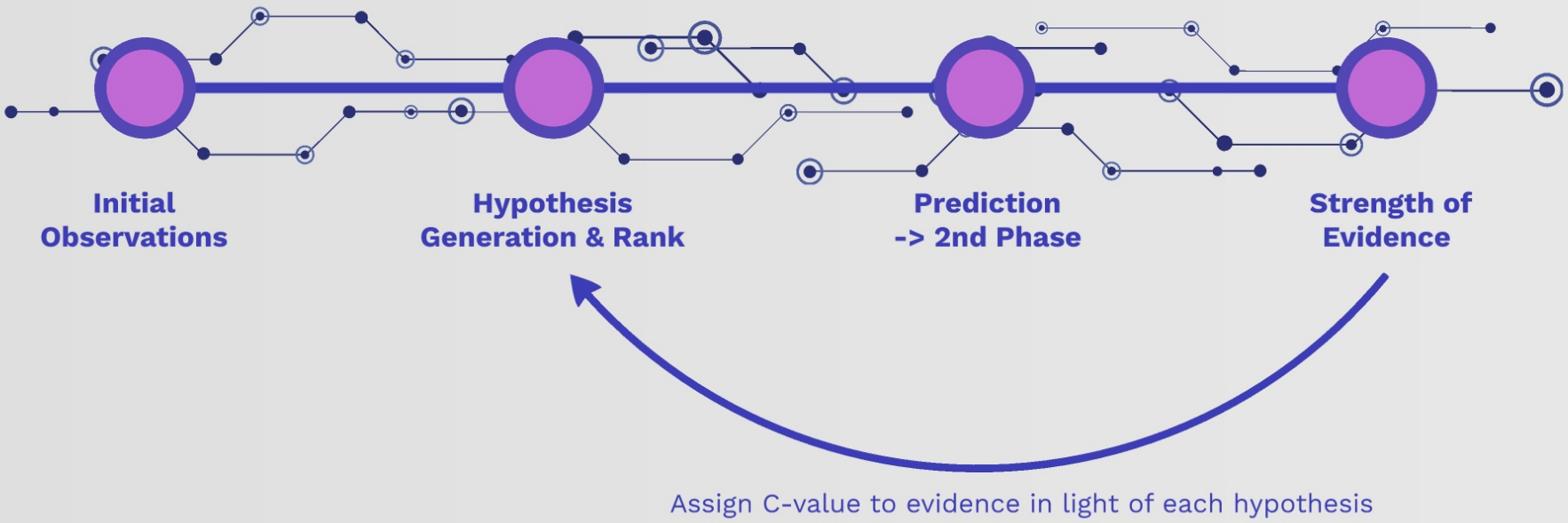
COMMUNICATION
Clearly conveying complex materials to diverse audiences

COLLABORATION
Working together builds trust & innovation

CREATIVITY & INNOVATION
Conceiving novel & innovative solutions

Revamping Scientific Practices

Case Assessment & Interpretation (CAI)



Case Assessment & Interpretation

Stage	Activities
1. Observation	**Make initial observations**
2. Hypothesis generation	**Generate a set of plausible hypotheses** (initial observations, case circumstances)
3. Inference to the best explanation	**Rank the hypotheses** (initial observations, current knowledge, past experience)
4. Prediction of likely observations	**Predict likelihoods for the range of possible future observations** (postulating that each of the hypotheses were true)
5. “Second Phase” observation	**Search for predicted likely observations**
6. Strength of evidence assignation	**Assign likelihood values to the observed digital evidence** (in light of each hypothesis / proposition)
7. Communication	**Express evaluative opinions**

C-Scale

C-Value	Illustrative Indicators
C0	Evidence contradicts known facts (extreme dissonance of observations in light of the hypothesis).
C1	Evidence is highly questionable (very strong dissonance of observations in light of the hypothesis).
C2	Only one source of evidence that is not difficult to tamper with.
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies (dissonance) in the observed evidence in light of the hypothesis.
C4	The source(s) of evidence are much more difficult to tamper with evidence from multiple, independent sources (strong harmonious observations in light of the hypothesis).
C5	The source(s) of evidence are very much more difficult to tamper with and evidence from multiple, independent sources (very strong harmonious observations in light of the hypothesis). However, small uncertainties exist (e.g. temporal error, data loss).
C6	The evidence is tamper proof (or tamper evident) and extremely strong harmonious evidence in light of the hypothesis unquestionable

Standardization of forming and expressing preliminary evaluative opinions on digital evidence (Casey, 2020)

Knowledge is Powerful

but ...

Access Builds Equity

Stories of 3 Interns

Supporting Equity &
Sustaining Diversity

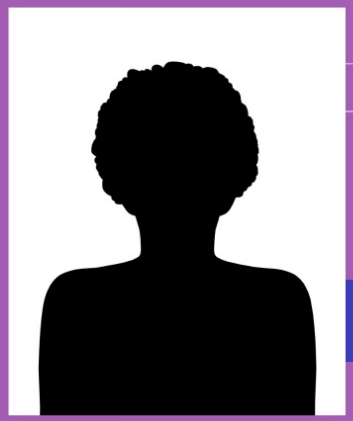
Intern 1

Intern 2

Intern 3

Intern 1

Single mom in New Orleans
Hadn't finished her HS diploma
Strong entrepreneurial spirit
Turned to ICT /DFIR career pathway
Working by day, studying nights and weekends

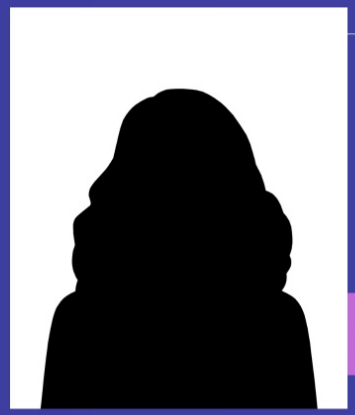


Graduated with honors

(now works in IT & education)

Intern 2

Returned to college while raising her daughter
Initially a Psych major but was encouraged to transfer to CS
Supported all IT systems in former job
(but without credit or compensation)
Discovered DFIR opportunities with DFS at a career fair

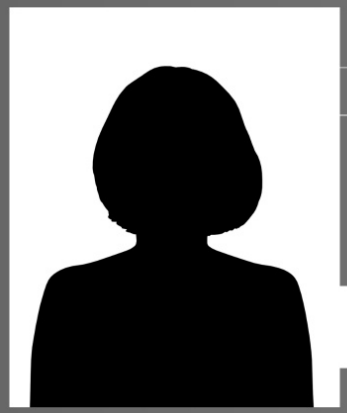


Completed CS Masters

(now a Senior DFIR lead at a multinational company)

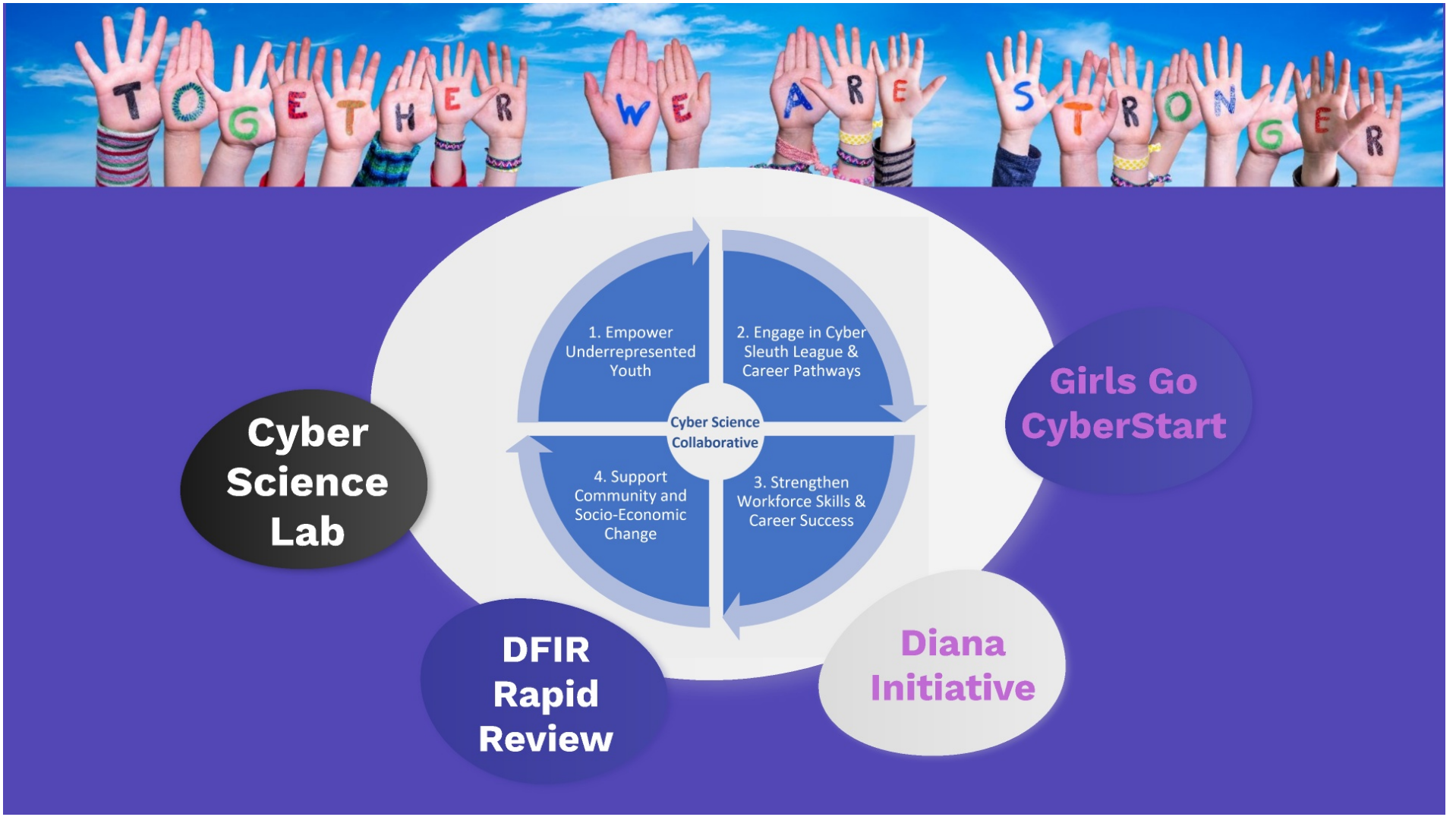
Intern 3

Enrolled in Design / Tech at community college
Started Internship as a "Digital Creative"
Engaged in design of Cyber Sleuth Science Lab
& coaching other young women in DFIR



Pursuing CS Degree

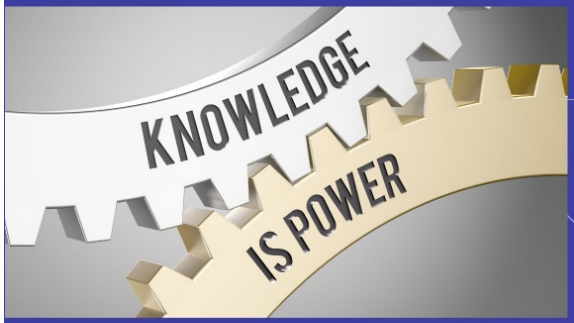
(focusing on DFIR and reverse engineering)


TOGETHER WE ARE STRONGER
1. Empower Underrepresented Youth
2. Engage in Cyber Sleuth League & Career Pathways
3. Strengthen Workforce Skills & Career Success
4. Support Community and Socio-Economic Change
Cyber Science Collaborative
Cyber Science Lab
Girls Go CyberStart
DFIR Rapid Review
Diana Initiative

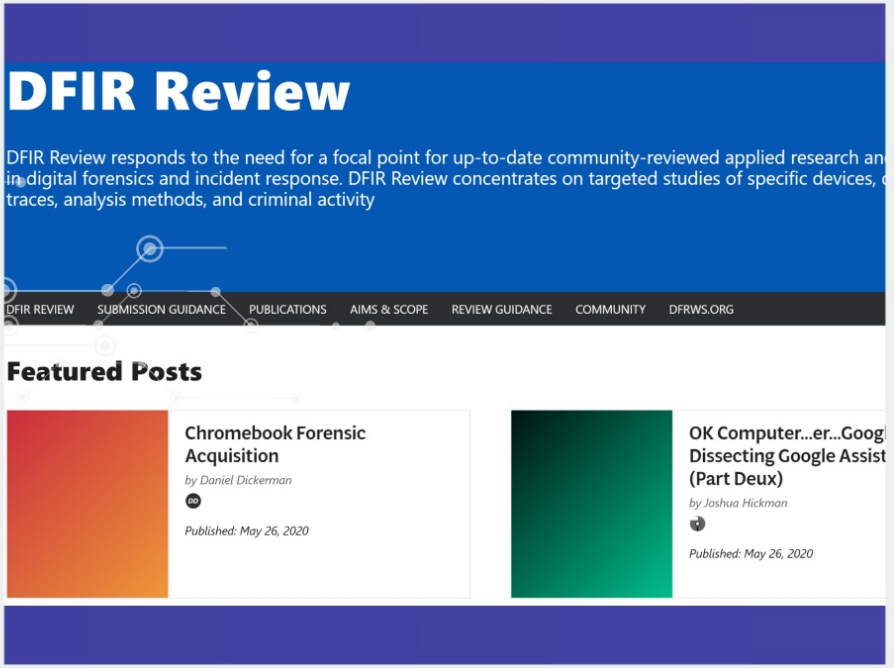
Cyber Science Lab

Inspiring underrepresented youth to pursue DFIR pathways

DFIR Review



Diversify publication



Diana Initiative

A conference focused on Women, Diversity, and Inclusion in Information Security

Girls Go CyberStart

Teaching girls DFIR via online games and competitions