ACSC2018
AUSTRALIAN CYBER SECURITY CENTRE
CONFERENCE 10 – 12 April | Canberra
acsc2018.com.au

Drinking from the firehose: rebuilding the forensic tool ecosystem

Bradley Schatz[1]
[1]*Schatz Forensic*

Traditional computer forensics is marred by unnecessary delays due to antiquated approaches to evidence storage and tooling. We set out to fix this by shifting the forensic tool ecosystem to a new file format, which enables forensic practice to scale to current data rates, and removes the traditional delay between identifying evidence and undertaking analysis.

This seminar will introduce the AFF4 forensic evidence storage format, and why is it is needed. We will outline our progress to date in growing the wider ecosystem of open source and commercial computer forensic tools. Along the way we will provide some surprising observations around the interplay of full disk encryption, modern storage systems, and forensic practice.