Evidence of anti-forensic activity has taken place on these new systems, and where it can be found is imperative. In addition, there is a lack of judicial precedent, statutory rulings, or legal interpretations on the admissibility and evidentiary treatment of anti-forensic activity. Our work bridges these concepts to provide practical guidance encompassing issues that arise with Windows 8 forensics, anti-forensics, and their respective legal concerns.

**Methodology:**

Two main phases of research:
1. Secondary research of prior forensic work, legal issues, existing laws and precedents.
2. Primary forensic research through experimentation.

The graphic (right) shows our methodology for forensic image creation.

**Findings:**

Key findings validated through forensic analysis:
- Artifacts persisted for all of the anti-forensic applications in several locations, including the registry, event logs, prefetch and jump lists.
- "InPrivate" browsing history can be recovered from several locations, including RAM and unallocated space.

Relation to legal research:
- Evidence of anti-forensic activity is indirect and its value needs to be assessed within a larger context.
- Volatile data acquired from a live system has a higher potential to raise admissibility concerns.

**Conclusions and Beyond:**

Common attempts to "cover one’s tracks" online are not very effective. Clearing browsing data, using "InPrivate" browsing, and executing applications designed to remove such evidence all fail at thoroughly doing so.

Evidence of anti-forensics may be used in court as evidence that the actor intended to commit the original charges. It can also be used as evidence for additional charges—obstruction of justice particularly-based on the anti-forensic acts.

Moving forward, it will be important to establish a formal set of overarching standards for the field of digital forensics. We should strive towards a framework based on legal requirements, which enumerates both industry and process standards for application developers and investigators.