

C:\> Actionable Evidence in the Wake of Anti-Forensic Activity on Windows 8 Systems _

Problem(s) :\>

Windows 8 and Internet Explorer 10 introduce a wide range of changes that are important to the digital forensic community. With that, an awareness of what evidence may remain after 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.

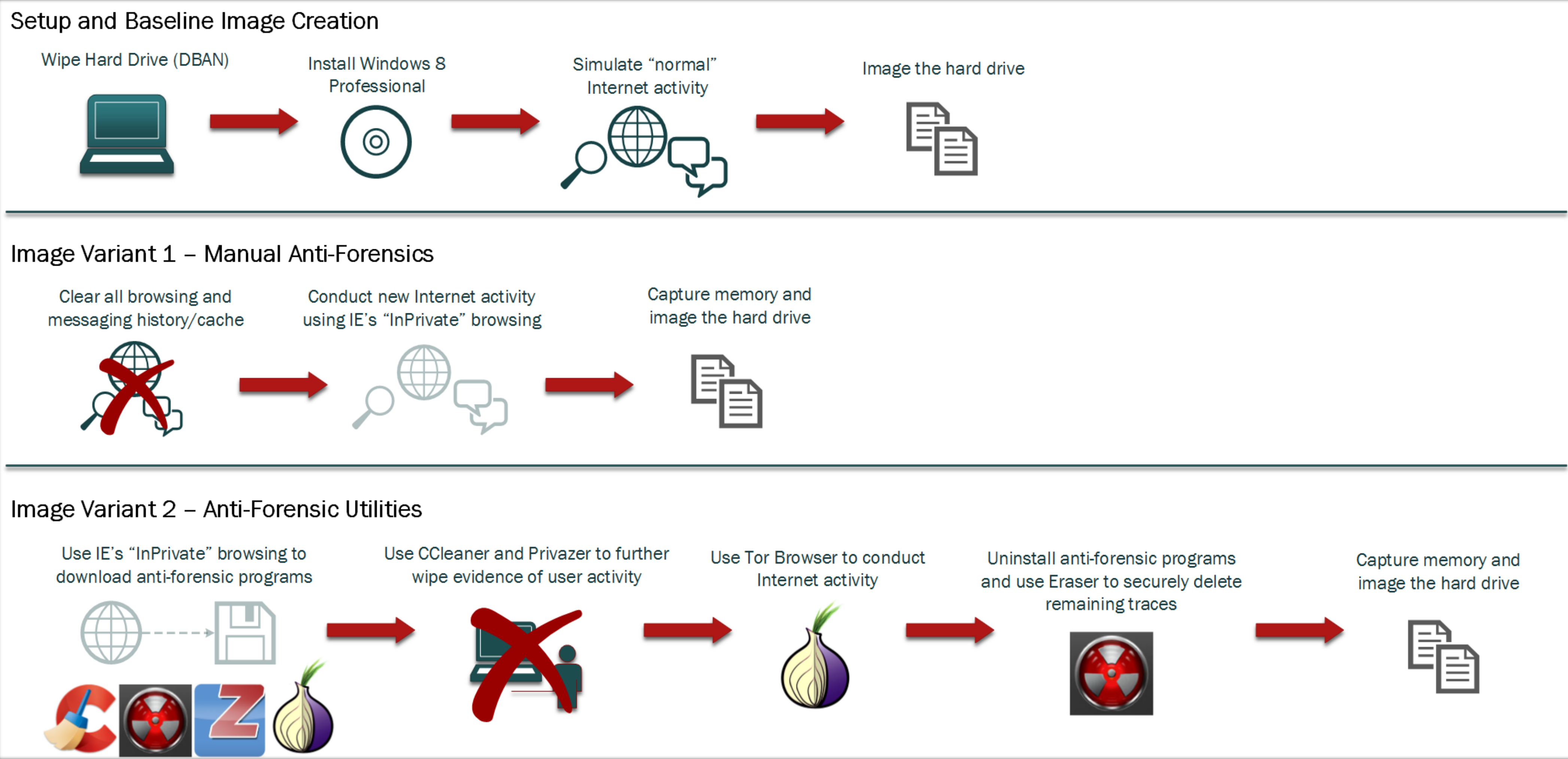
Our work bridges these concepts to provide practical guidance encompassing issues that arise with Windows 8 forensics, anti-forensics, and their respective legal concerns.

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.



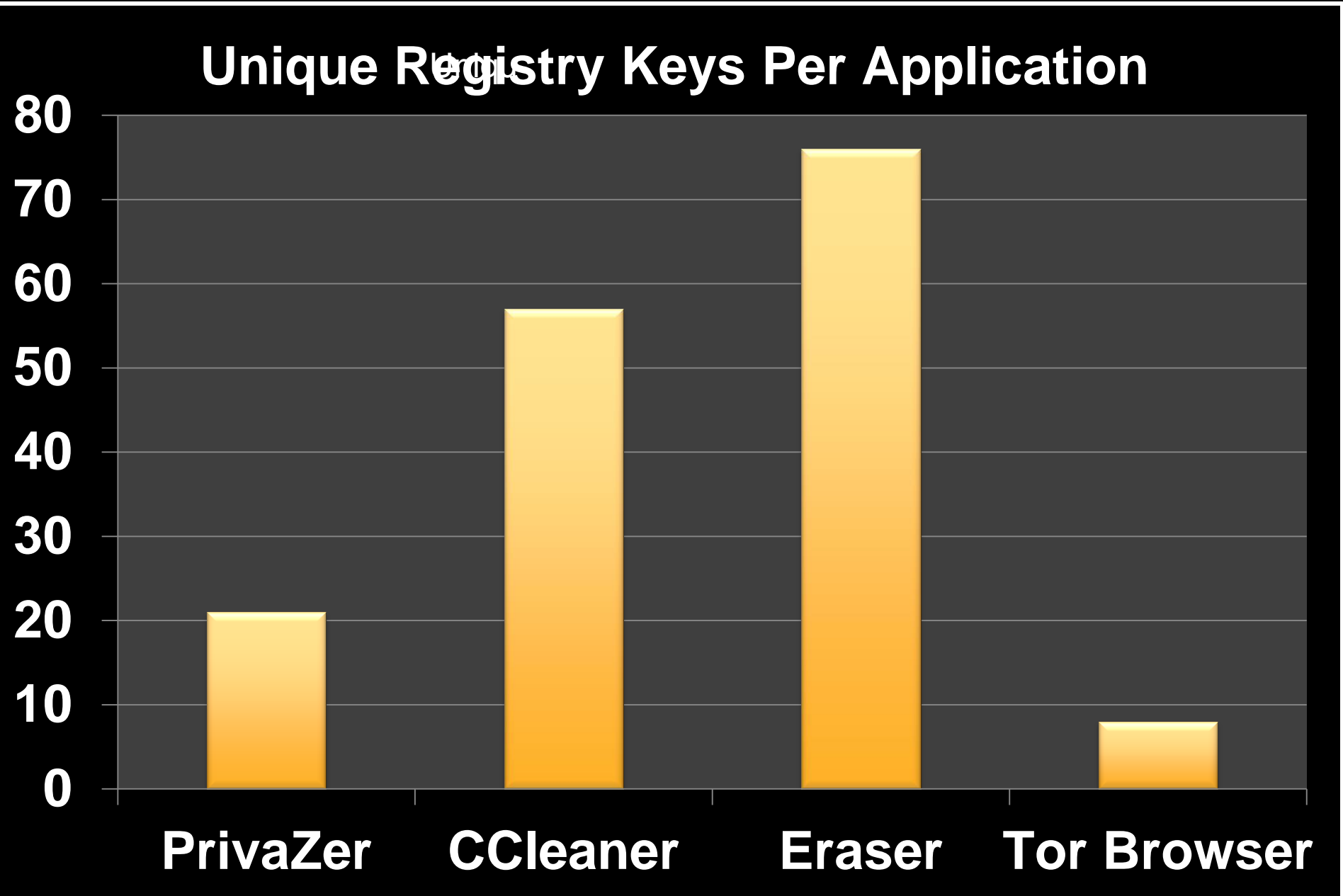
Findings:\>

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.



← Chart showing counts of registry keys found in Image Variant 2 for each of the anti-forensic applications used. These are keys that persisted after uninstalling the respective applications.

Changes to WebCacheV01.dat Containers				
ContainerId	Baseline	Variant 1	Variant 2	Name
1	95	1	49	Content
2	176	3	X	History
7	9338	9117	N/A	iecompat
11	130	2	3	Cookies
12	371	X	N/A	History
13	3506	20	N/A	Content
15	4	2	4	Cookies
16	7	1	X	iedownload
18	23	X	N/A	DOMStore
24	1	1	N/A	DOMStore
25	8	8	N/A	Content
26	X	X	N/A	Cookies
27	75	6	14	Cookies
28	157	1	X	History
29	1560	107	N/A	Content
30	78	78	N/A	MSHist012014031720140324
31	25	25	N/A	MSHist012014032420140325
32	12	1	1	DOMStore
33	36	36	N/A	MSHist012014032520140326
36	10	10	N/A	MSHist012014032920140330
37	N/A	4	N/A	MSHist012014033020140331
38	N/A	X	N/A	MSHist012014033020140331
39	N/A	X	N/A	MSHist012014033020140331
40	N/A	X	X	iedownload
41	N/A	N/A	4	MSHist012014032420140331
42	N/A	N/A	X	MSHist012014033120140401

← Spreadsheet showing counts of records in the WebCacheV01.dat "Containers" for each image. Yellow indicates counts that were diminished from one image to the next while red indicates containers which were entirely deleted.

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.