DisputeSoft
Software Dispute Experts

What Every Attorney Needs to Know about Computer Forensics, Part 3: What Criminal Defense Attorneys Need to Know about Computer Forensics

G. Hunter Jones | Managing Director & Forensic Examiner

When our computer forensics experts are engaged on a criminal case, our client is almost always counsel for the defense.

Most law enforcement jurisdictions have in-house Computer Forensics specialists; thus most of our forensic engagements come from defense counsel rather than the prosecution. Thus, most of the work performed by our Computer Forensics experts is directed toward rebutting or challenging evidence presented by the prosecution.

Evidence derived from Computer Forensics can come from a wide array of sources – computers, tablets, smart phones, cameras (including surveillance cameras), GPS units, cell towers, or any other digital device that tracks and retains information about its user or its user's activities.

Evidence derived from Computer Forensics can come from a wide array of sources – computers, tablets, smart phones, cameras (including surveillance cameras), GPS units, cell towers, or any other digital device that tracks and retains information about its user or its user's activities. This information can be used to show where a person was at a specific time, what the person searched for, looked at, or took pictures of, who the person corresponded with and what he/she said, and, in the case of surveillance footage, exactly what a person was doing at a specific time in a specific place. TV crime shows usually tell us how such information is used by law enforcement to find and convict perpetrators, but sometimes such evidence can aid the defense by demonstrating, *e.g.*, alibi, or rebutting the prosecution's theory by showing that it has misinterpreted the forensic evidence.

In many cases, the best defense-related evidence comes from data overlooked or misinterpreted by the prosecution. Consider the following situations, which DisputeSoft forensic experts regularly encounter during their investigations:

- Alibi evidence – At the time of an alleged robbery, the defendant was online at his home computer updating his own website, adding material clearly of his own theme and style. Capturing this evidence from his computer and from the website showed that he was posting those updates and not committing the robbery at the time in question;

- Alibi evidence – During the evening of a charged assault, usage and activity data in the alleged victim's laptop showed that she was so busy with online games, social media, and e-mail that there was no time at which she could have been attacked as claimed;

- Interpretation of evidence – The prosecution relied on cell-tower data to show that the defendant was in the vicinity of the crime. However, an independent review of the data showed that the prosecution's cell tower analysis ignored the sector information, which shows in which direction the user of the phone was located from the tower. In fact, while the cell-tower data shows that the defendant was in the vicinity, it also shows that that the he was in a sector well removed from the specific site of the robbery.

When the defense needs to rebut or challenge forensic evidence presented by the prosecution, analysis by a computer forensics defense expert can provide essential information about a person's activities and location at a particular date and time.

However, more often than not, the prosecution's forensic digital evidence is compelling, and the defendant is far more likely to be convicted than he has recognized. In such cases, the forensic defense expert's greatest value is in assisting defense counsel to understand the forensic evidence and how it is likely to be seen by the trier of fact. Sometimes, the greatest value of the defense expert is to assist defense counsel in persuading the defendant to seek a reasonable plea, rather than going to trial.

DisputeSoft has been involved in such an outcome on a wide range of criminal cases, such as cases involving collecting and trafficking in pirated movies (and similarly with child

pornography), creating a false identity on social networks to use in seeking underage partners, and destroying digital evidence in order to conceal illegal activity.

Read Part One: What is Computer Forensics?

Read Part Two: The Difference between Electronic Discovery and Computer Forensics

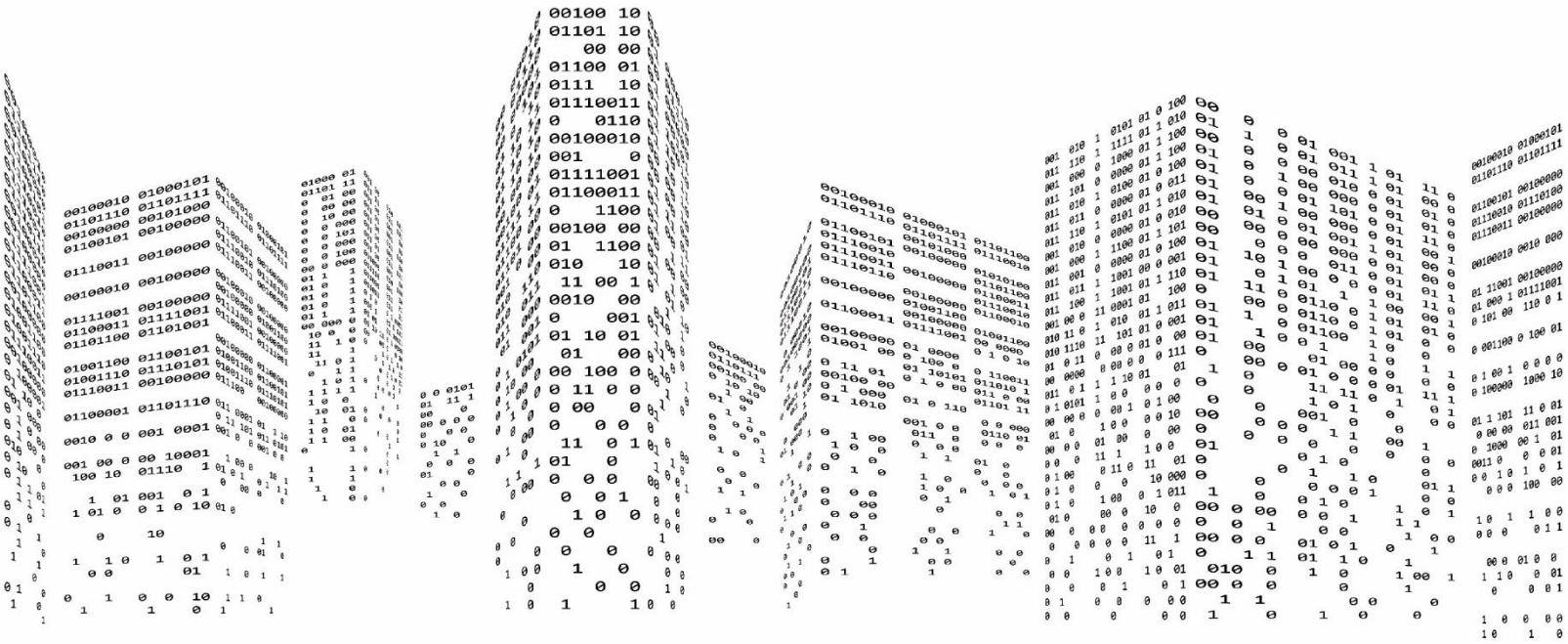
Read Part Four: What Trusts and Estates Attorneys Need to Know about Computer Forensics

---

G. Hunter Jones

Managing Director & Forensic Examiner

Hunter Jones has over 40 years of experience as a systems engineer, working in IT consulting and computer system development. As a systems developer, he is intimately familiar with the internals of computer systems, both operating systems and application programs. As a certified computer forensics specialist (EnCase Certified Examiner and GIAC Certified Forensic Examiner), Hunter has established credentials in the fields of computer forensics and electronic discovery. Hunter also has deep knowledge of computer forensics as it relates disputes concerning medical malpractice, video files, patent infringement, and internet misconduct.



If you are an attorney in need of a computer forensics expert, we invite you to consider DisputeSoft.

Contact Information

Jeff Parmet, Managing Partner

301.251.6182 | jparmet@disputesoft.com

12505 Park Potomac Ave. | Suite 475 | Potomac, MD | 20854