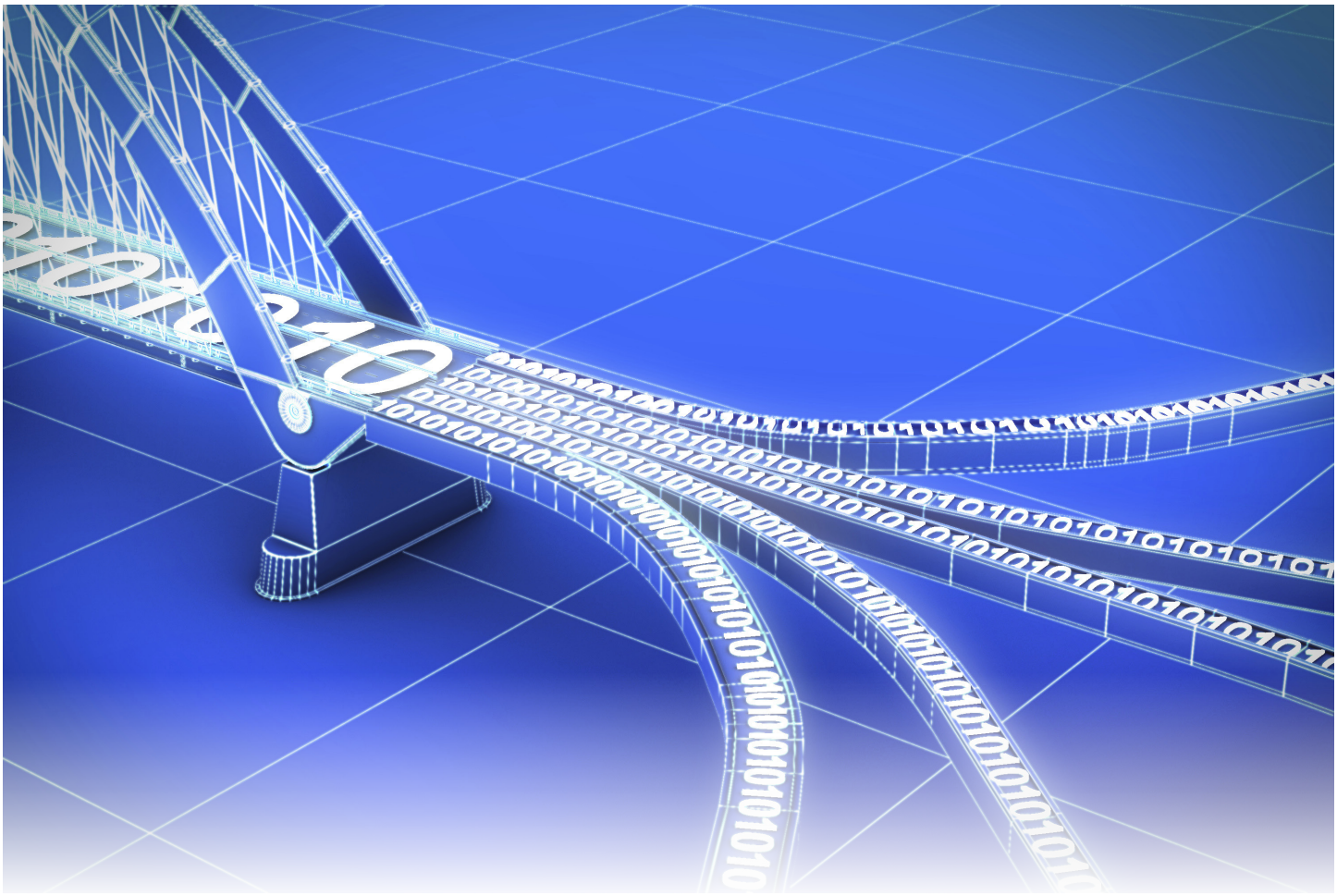
Delving Into the Client's **Data Architecture**

PART 2 OF 2: SURPRISE WITNESSES



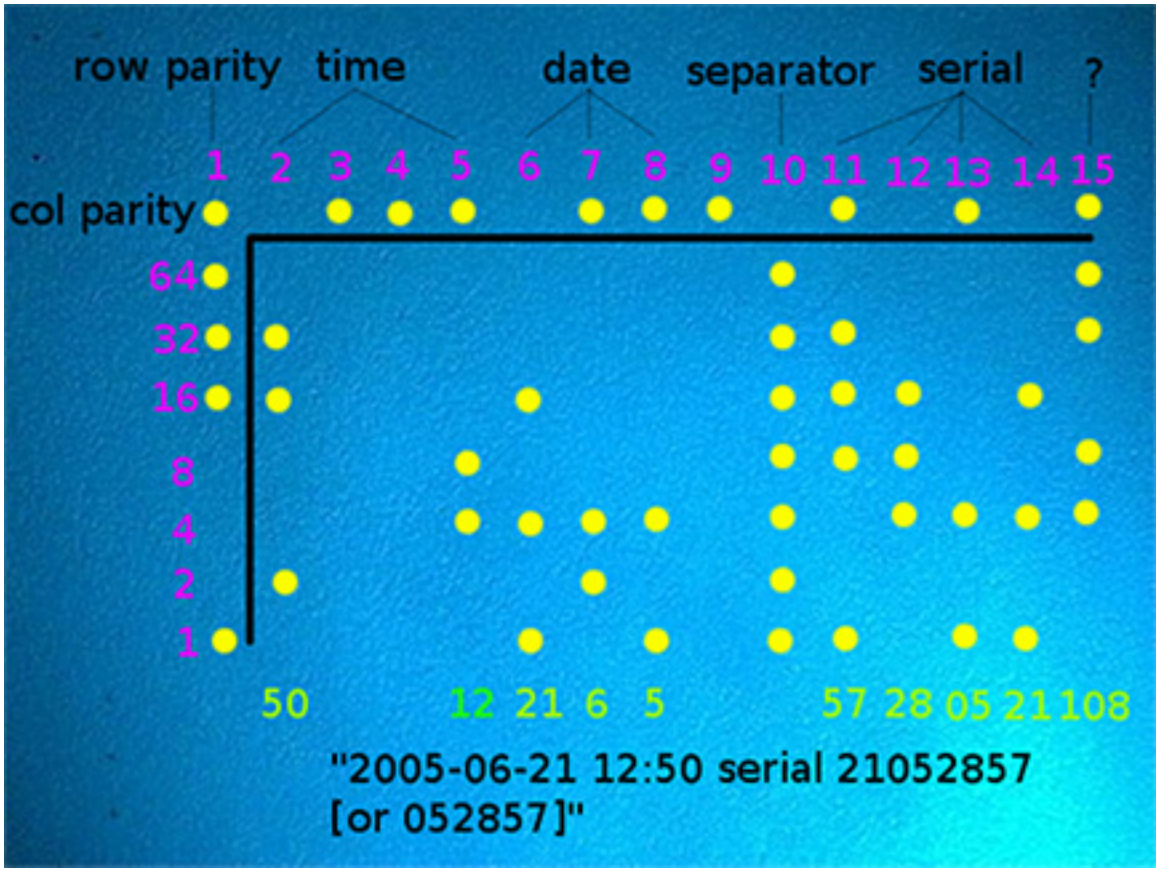
WHITE PAPER

VESTIGE
Digital Investigations

Preservation is Key to **E-Discovery**

Many attorneys may recall one or more favorite television shows in which a clever defense attorney "springs" a surprise witness on the prosecution. The results are usually the dramatic collapse of a case, or the confession of a third party and the exoneration of the accused. This type of "Deus ex machina" has become a fairly common feature of electronic evidence; primarily because most human beings have no idea of the manner in which our electronic devices work. As a result, our devices frequently become a type of "surprise" witness.

Not every electronic witness will be a computer. Even the simple color copier can become a powerful witness. Color copiers have become "event witnesses" in certain cases because color copiers secretly embed onto each color copy certain anti-counterfeiting data that identifies the make, model, and serial number of the color copier, as well as the date and time when the copy was made. In one such case, certain criminals used a color copier to created counterfeit rail tickets. The counterfeit tickets were circulated and ultimately attracted the attention of the Dutch police. The police, however, knew that many color copiers can become event witnesses by analyzing the anti-counterfeiting dots.



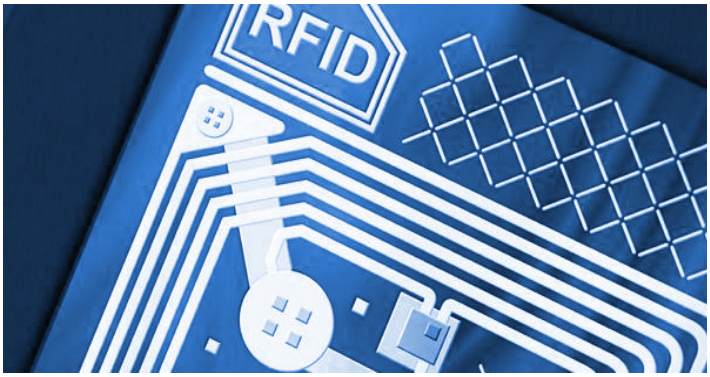
Above is an example of anti-counterfeiting dots embedded in a copied page.

By examining the counterfeit ticket, locating the embedded anti-counterfeiting dots, and interpreting those dots, the Dutch police quickly obtained the copier's make, model, and serial number. It was relatively simple, thereafter, to locate the purchaser of the copier and subsequently arrest the people responsible for the counterfeit tickets.

This example highlights the usefulness of treating an electronic device as a witness, even when the exact manner in which the device operates is not known. Treating all electronic devices as if they were potential witnesses in a case is very similar to treating people at the scene of an accident as witnesses.

Electronic Devices as Witnesses will not always be visible or obvious

Electronic Devices that are also witnesses will not always be visible or obvious. Radio Frequency Identification Devices, for example, are frequently smaller than a grain of rice and may be embedded into equipment, tools, and identification tags, etc. Consider a hypothetical case involving a claim that a patient was left lying in a bed, unattended for several hours in a hospital corridor, where he eventually died. Counsel interviewing the hospital client ought to be able to identify the key players, including the on-duty nurse, doctor, and any witnesses that saw the patient in the corridor. Using the three step, Computer as Witness Paradigm, counsel ought to expand beyond the identification of key players to include the electronic devices used by each key player. In order to identify the electronic devices, Counsel ought to interview the IT personnel and create a matrix as described above. During this interview, counsel ought to constantly probe IT personnel's characterizations and representations to be certain that counsel understands the data architecture used in the hospital. In this hypothetical, the attorney ought to identify security cameras that record electronically



the corridor in question and any RFID (radio frequency identification device) embedded in the patient bracelet. When used to track patients, RFIDs in the patient bracelet communicate with an "interrogator" device to log the location of the bracelet. These tracking logs area stored on special servers, and can be provided to counsel. By reviewing these logs, counsel will be able to track the patient's movements throughout the day; and will be able to prove that the patient was never in the corridor unattended for several hours.

In addition to tracking patients by bracelets, RFID technology is being used to track doctors and nurses. RFIDs embedded in employee identification cards permit employee tracking logs to be created and maintained for all employees—including those key players that claim to have seen the patient in the corridor. Their testimony can be corroborated by proving that the RFID logs locate the key player at the precise place and time as their oral testimony.[ii]

Counsel need not completely understand how the RFID device works, nor does counsel need to know the exact electronic evidence resident on the device (or on the computers to which the device communicates). Rather, Counsel can get technical help where needed to preserve the device and search it to recover evidence at a later date. ◊

[i] *http://www.pcworld.idg.com.au/index.php/id;1002274598, "Dutch Track Counterfeits via Printer Serial Numbers".*

[ii] *See, for example, The Ohio State University, "RFID Hospital Patient Tracking" as part of the Patient Tracking Netwiser Project, Fall 2008 available at https://ceti.cse.ohio-state.edu/ceti/showcase/bitwiser.*

VESTIGE
Digital Investigations

For more information Contact us today
800.314.4357 or info@vestigeltd.com