

LJNLAW JOURNAL
NEWSLETTERS

LJN's

LEGAL TECH

Newsletter®

An **ALM** Publication

Volume 32, Number 9 • January 2016

**Catching
Counterfeiters
With Page Vault**By **Rob Holmes**

As the CEO and founder of IPCybercrime, my team and I have developed a systematic approach to investigating the online sale of fake branded goods. We work with law firms and corporate counsel to build cases against the counterfeiters. In the last decade, we've assisted in shutting down hundreds of thousands of websites offering counterfeit goods for sale. In many cases, \$100s of millions were at stake.

This article discusses how we build a case against counterfeiters and a new tool we've found, Page Vault, that is helping us to do this more effectively.

CATCHING COUNTERFEITERS

In 2010, the Second Circuit determined that brand owners are responsible for monitoring the infringement of their trademarks. See, *Tiffany Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010) (<http://bit.ly/1MaUrDr>). This is where we step in. Multiple courts have relied upon the results of our investigations — finding in favor of plaintiff brand owners such as Louis Vuitton, Chanel, Microsoft, Gucci,

Rob Holmes is the founder & CEO of IPCybercrime.com. He has conducted some of the world's first IP-related Internet investigations, and pioneered the study of the "virtual crime scene."

To learn more, visit ipcybercrime.com



and others — and our investigations have figured prominently in landmark cases. We've been proud to play an innovative role in developing techniques to catch online counterfeiters.

Counterfeiters take advantage of the quickly evolving nature of the Web to stay one step ahead of authorities. We keep up with them by developing our own tools in-house and by partnering with state-of-the-art companies so that we have the best toolkit in the industry.

Counterfeiters manufacture replicas of branded merchandise (e.g., fake Louis Vuitton, Gucci, etc.). Then they sell these knock-offs online at a discount. To sell, they use either online marketplaces (eBay or Ali Baba, for example) or set up their own domains to sell the goods (gucci4less.com, for example). These are large, sophisticated operations, so we need to be more sophisticated to catch them.

The International Chamber of Commerce (www.iccwbo.org) estimates that the global value of counterfeit and pirated goods in 2015 was between \$770 billion and \$960 billion, and that G20 economies lost more than 2.5 million jobs as a result.

Counterfeiting is a "white collar" crime built around a sophisticated business model. The aim of our investigation is to determine the pattern and intent of the counterfeiters' activity across all of their websites. To establish this pattern, we carefully gather evidence about their online activity and get actual examples of the counterfeit goods.

FIRST RESPONDERS

The first thing we do is perform a WSA (Website Analysis) of a counterfeit sales site. We approach the WSA as if we were first-responders to a crime scene — CSI for the Web. CSI has rules for "opening up" a crime scene, from making initial photographs to taking fingerprints, gathering and tagging crucial evidence, and finally "closing" the crime scene. We've developed our own set of best practices for doing this on the Web.



We make digital copies of each and every page; we also gather the IP address, the DNS, and the "Whois" information (key information about the ownership of the Web page). Collecting the source code is also very important. It's crucial to do all of this at the start of an investigation; counterfeiters move very quickly, so if you come back even a few hours later a page may be changed or gone.

SCREENSHOTS AND SOURCE CODE

More and more cases are being won with screenshots and source code. Making screenshots quickly, documenting them properly, and also getting source code is a massive technical hassle.

Our investigation supported the landmark *Chanel v. Dror Krispin* case in 2008. See, *Chanel v. Dror Krispin*, 1:2008cv23439 (F.S.D.C. 2008) (<http://bit.ly/1LkswAk>). Chanel won the case because of screenshots and captured source code. The counterfeiters operated a lot of apparently unrelated websites. We proved that the sites were related by matching Google analytics codes embedded in the Web pages' source code across different counterfeit sites. We pioneered this method, which has become a standard way to establish pattern and intent, and the true extent of counterfeit activity.

Gathering copies of the page is time-consuming. First, simply printing the browser page doesn't work very well; the printout often doesn't look exactly as it appeared in the browser. Second, counterfeiters often protect themselves by adding elements to the CSS code on their site (the "style sheet") that prevents the page from printing, or prints unrecognizable versions of the page. If this happens, our investigator needs to make a screenshot of the browser, then scroll the page down slightly, make another screenshot, and so on, until the entire page is captured. Very time consuming.

USING PAGE VAULT IN OUR WSA

This year, we discovered a new tool that has become a central piece of our WSA workflow — Page Vault. The main purpose of any investigative tool should be to eliminate technical hassle in an investigation. Page Vault was built exactly to do this — it saves us time in capturing any Web page and specifically maintains the digital chain of custody for evidence.

Page Vault is software that captures screenshots, source code, and metadata of Web pages, automatically documents them, and authenticates them for legal use. It is extremely easy to use, and the "team" plan enabled everyone on my team to work at once on an investigation without extra cost.

Page Vault appears as an ordinary browser with an additional button to "capture" the Web page in view. Page Vault automatically scrolls the page and screenshots every part of it. Page Vault stores the captures online as a PDF, with a record of the metadata (URL, IP, date, and time of page load and capture) on the first page. Page Vault also automatically saves the source code at the same time.

The usual CSS tricks used by counterfeiters to prevent printing of the page through the browser don't work against Page Vault. We like that the PDF shows the Web page exactly as it appeared in the browser.

Previously, we would scroll and screenshot each website manually, save the source code separately, copy-and-paste the URL, and look up the IP address, and then make sure everything was stored together. Page Vault accomplishes all of this in seconds for a given Web page. The time savings is big: a sophisticated counterfeiting operation may be running hundreds or even thousands of pages.

MAKING TEST BUYS

"Test buys" are undercover purchases of counterfeit goods. After our initial WSA,

we need to "get the goods." We set up each of our investigators with an undercover ID, including a PayPal account and credit cards. Then, the investigator documents each step of the purchase. We use Page Vault as our browser for the test buys because we need to make a screenshot of every single page in the purchase process. We capture every page all the way through the PayPal receipt in our e-mail, the tracking numbers delivered to our e-mail, and even the USPS tracking website.

CHAIN OF CUSTODY

Page Vault also preserves chain-of-custody for legal purposes; this sets it apart from free or over-the-counter screenshot applications.

The defendants in counterfeiting cases know that the stakes are high and will do anything possible to derail a case; haggling over Web page evidence is a great tactic.

I have been questioned in multiple depositions about the integrity of our handmade Web page captures; whether the dates, times, and IP addresses were properly recorded, and how I can prove that my evidence accurately reflects how the page actually appeared.

Deposers know that I have the expertise to produce screenshots that show something other than what actually appeared. While I would never risk my professional reputation by doing so, both sides know that stakes in a case are high enough (tens of millions of dollars in higher profile cases) to warrant caution.

I answer based on my reputation as a professional and expert, and I have to go into great detail about the documentation process. Testimony from me and my investigative staff has also been required, stating that our captures faithfully represents what was on the Web.

Page Vault's browser is hosted on a remote server, and my access to a Web page on it is limited to surfing and capturing. I view and operate the browser via a remote connection, which provides the look and feel of a standard browser. So when the Web page loads to the Page Vault browser (on their server), I see it remotely, and when I hit capture, the Web page and source code is captured, hashed, and digitally time-stamped for authentication; all within their system.

So Page Vault is acting as a "Trusted Third Party," and I cannot be accused of manipulating the capture, mistakenly recording the associated data (time, date, URL, IP address), or of changing it later. Page Vault provides affidavits

on request that detail its process so the court can understand that the captures are sound.

When we are working with clients, we explain this to them for discovery purposes to impress upon them that we are using state-of-the-art tools and are not putting their case or brand equity at risk.

Having assurances like this can knock an hour or more off a deposition and saves a lot of headaches.

INCORPORATING RESULTS

In the early 2000s, we realized that we were gathering a growing amount of documentation of Internet anti-counterfeiting cases. We developed the LitPak (the "litigation packet") to compile all of the information into one electronic document to make our clients' lives easier. LitPak is our forensically sealed report that is our deliverable for our clients. LitPak is presented as one comprehensive PDF document. We now incorporate Page Vault PDFs into nearly every LitPak; its use of the PDF standard for electronic document delivery fits well with our workflow.

THE FUTURE

We've worked closely with Patrick Schweihs at Page Vault, who is himself an IP attorney with an anti-counterfeiting background, so he understands our needs. The team there is responsive and interested to hear about how we are using the product and how it can continue to improve the product.

Page Vault has several forthcoming features that are designed specifically for anti-counterfeiting. We appreciate that they understand the anti-counterfeiting space and are continuing to build the product with us in mind.



PAGEVAULT[®]
THE INTERNET AS EVIDENCE
page-vault.com

