UnitedLex

The Smoking Gun: Evidence, Discovery, and Digital Forensics

A Case Study on the Difference Between Winning and Losing in Complex Litigation

Introduction

"The recent ruling in the Red Wolf case completely underscores the fact that the judge expects the attorneys and the experts to display a true technological competency as they are dealing with all the digital evidence in a case."

In the matter *Red Wolf Energy Trading, LLC v. Bia Capital Management, LLC, et al.*, Senior U.S. District Court Judge Mark L. Wolf entered a default judgment against the defendants and granted a second motion for sanctions. The case brought to light an unprec-edented, yet critically important judgment for modern-day litigators. This decision shines a strong spotlight on the need for practitioners and their clients to under-stand today's digital technology trends and to carefully select their partners when exploring communications across an ever-expanding list of channels.

This interview is with two of the leading experts at **UnitedLex,** Derek Duarte and Colleen Freeman, hired by the law irm Armstrong Teasdale to help expeditiously review the discovery exchanges and determine what data was missing from the documents provided by the defendants. The discussion includes detailed guidance to navigate digital communications, strategies to select an electronically stored information (ESI) partner for these types of complex litigation cases and a deep dive into the role data scientists and legal practitioners can play in this landscape.

Derek, how did you become involved in digital forensics?

Derek: Back in undergraduate, I took an internship with the Berkeley City Attorney's Office. And because I was young and had experience working with computers, they put me on all their eDiscovery matters.

One of my first experiences was on a case that involved the relevant date range from *1860 to 2000* regarding who built a portion of Berkeley's underground infrastructure and whether or not the city had maintained it and integrated it into the infrastructure. It was interesting, because I learned how to search e-mail systems and pull data from those systems, as well as how to search archived warehouses and paper record-keeping systems. And that really helped formulate my approach to how I look at this data in cases that I am involved with, even now.

In this case, I was able to find an old paper letter from 1927 that broke open the case during the course of the review. And that's what made me go to law school and really, where I got the taste for this type of work. And, more and more often, clients would ask me: how would you prove this? How would you figure this out?

I kept using that same approach over and over again, and eventually, I went and got certified as a forensics expert through Global Information Assurance Certification (GIAC), and I also sit on their Advisory Board. For most of these cases where I have been involved, I have been asked to testify on these types of trade secret matters.

Colleen, how did your career progress as an eDiscovery consultant?

Colleen: I had a very early interest in entering the field of law. While attending Boston College, I sat on the Student-Faculty Judicial Board which dealt with alleged violations of the Student Code of Conduct. This fueled my interest in wanting to pursue a career in the law.

Through my work in the compliance department at Fidelity Investments, I fielded inquiries from regulatory bodies and federal agencies such as the National Association of Securities Dealers (NASD) and the Securities and Exchange Commission (SEC). My department was also responsible for overseeing the employee trading gate, and even back then, our ability to uncover fraud and detect employee noncompliance with trading really was an interest for me. I also worked at a national accounting firm to help them build out their forensics, litigation, and valuation services line in Boston. This is how I got involved in eDiscovery early on, well before we started putting the "e" in eDiscovery. It was an exciting time as the firm was in the process of building out their eDiscovery service line and their own evidence lab in Texas. I got in on the ground floor and it helped me to think about discoverable information and the detection of fraud in new ways.

In my work, teaming up with our forensic experts like Derek and our data experts adds tremendous value. Not only do I bring a lawyerly perspective, looking at the case from all the important angles, but I also look at the case from a true eDiscovery

perspective. By having that strong foundation in eDiscovery best practices, I can advise clients on what to do, what not to do in eDiscovery, and the dangers around self-collecting, which has been coming up quite a bit in some of our cases.

How did UnitedLex end up working with Armstrong Teasdale on this particular matter?

Colleen: My work in this case dates back to 2019. John Sten reached out to me (currently an Armstrong Teasdale Partner and Boston Office Managing Attorney) when the case was first filed and asked if I could help out on the case. During the early phase of discovery, I was hired to assist with the plaintiff's collection efforts, devise the review methodology and oversee a team of reviewers. Due to some of our early successes in the case and my long-term client relationship with John, he sought me out again to help fight these egregious discovery abuses. This is a great example of the power of a strong client relationship. They can achieve greater successes when partnering on these matters and allow us to be a true trusted advisor.

One thing we want to underscore in this matter is that *Red Wolf's* counsel was only given 5 days to retain a forensic expert, analyze the Slack archive and file an affidavit documenting the expert's findings. That's when our team at UnitedLex was hired to help counsel meet the considerable challenges in the case and execute on such a tight timeline.

John needed my help with determining which forensic expert would be best suited to perform the Slack analysis and report their findings. I knew if anyone could help us quickly with reviewing the Slack archive and uncovering any anomalies it would be Derek Duarte.

Derek and I worked the entire weekend with an expert team of data analysts to get this right for our client. We understood the critical need to replicate the workflow and perform a detailed forensic analysis of the old Slack archive. I am especially grateful that our entire UnitedLex team brought a contagious positive energy and really rolled up their sleeves for this client.

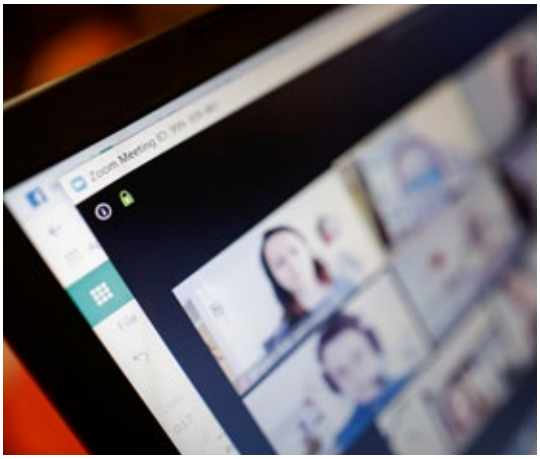
This litigation battle and the astonishing outcome underscores the importance of delivering for our clients as well as understanding the latest legal applications for digital technologies. In this case, it resulted in a significant victory for the firm's client.

What impacts will the post pandemic, remote-first environment have on cases like these? Do you anticipate they will increase in frequency and scope?

Colleen: Since the pandemic started, there has been a growing dependency on eDiscovery professionals. One major new challenge that our clients at UnitedLex are facing is how to manage the proliferation of chat communications and emerging data sources. By all accounts, chat communication tools appear to be replacing email for corporate communications. This is presenting new challenges for our clients and their outside counsel when faced with responding to discovery requests.

During the pandemic, the entire world stayed in touch through Zoom, Teams and other video chatting platforms like FaceTime. These virtual interactions helped us all feel connected during the shutdown and created a dramatic shift in how we communicate both personally and professionally.

The standard reliance on corporate communication channels like email is starting to decrease, even becoming obsolete in some cases, as employees are more and more moving to less formal channels to communicate—like video conferencing, chat, and text—in the post-pandemic, hybrid workplace. The need for lawyers and experts with technological competence to manage these communication channels successfully, to reconstruct conversations across multiple communication vehicles, is on the rise. Conversations may begin in e-mail, then move to text, and then continue on a call. After the call, they might move right back into text or use a chat messaging platform like Signal where their instant messages are encrypted.



This all poses a challenge for litigators today who are tasked with reconstructing important communications in response to discovery requests. This work now requires a higher degree of digital and technological competence. In fact, most states now require attorneys to keep up with technology as part of the "duty of competence." Today, attorneys have a "duty of technology competence" and are expected to understand how technology may affect their case and their client's legal discovery obligations.

"Red Wolf's counsel was only given 5 days to retain a forensic expert, analyze the Slack archive and file an affidavit documenting the expert's findings. That's when our team at UnitedLex was hired to help counsel meet the considerable challenges in the case and execute on such a tight timeline."

I think we're going to see, with the exploding data volumes, a growing dependency on the expertise that Derek, myself and our team of data experts can bring. Lead counsel's selection of these types of experts could make a critical difference in whether you succeed with your claims in court or whether you're going to get embroiled in discovery disputes and possible motions for sanctions.

Derek: I would say it has definitely increased in frequency and scope because of the pandemic, as organizations focus on allowing everyone to get their work done and at the same time, being secure. And so, it is very fragmented with a lot of communication systems. There's a huge uptick in the use of these collaborative messaging systems and the need to analyze them. I don't think it's going to continue to grow from where it is now though. I think it's kind of at its peak, and security teams need to figure out how to manage this securely.

The legal practice itself has not caught up to where the IT and security industry is today, still looking at e-mail or word documents. On the *Red Wolf* case, you can see how the other side treated Slack here. They're not really thinking about these new tools in the framework of "how does it work?" and "how is it actually used?"

What pitfalls should ESI providers look for in these cases? Are there any common red flags to avoid?

Derek: I think they need to know that discovery really is about determining facts right and surfacing evidence. And so, playing "gotcha eDiscovery Games" is, I think, going to be severely punished. This Slack case is the beginning of judges reacting, because you have a huge informational advantage. With all these chat programs, it's easy to be disingenuous and hide the ball. And that's not at all what the spirit of discovery is all about.

It's all about diligent search and reasonable inquiry or variations of that concept and then sharing information with the other side so that you can litigate it. And I think a lot of people have used this technical complexity to play "gotcha games" in the discovery process. I think, if you know something happened, and you're trying to figure out a way to play a gotcha game, you have to be wary of that – that's not the strategy here.

In addition, be very wary of vendors who are selling, what I like to call, "magical dust artificial intelligence (AI) solutions." It's impossible to say, "I'm going to throw in all my Slack, all my text messages, all of my documents and all of my emails, and we're going to have the answer of what should be responsive, what should be privileged and whatnot." That's not how Discovery works. The tech can't do your job for you. Providers and their experts really need to think about what actually needs to be determined in this case.

And then you have experts both in how the company works and how the data works who provide a reasonable answer and a reasonable production. You need to stay focused there, and if your process doesn't involve that, no AI tool can plug that gap.

Colleen: I believe this case raises an important issue in our industry that has long been a subject of debate, namely the overreliance on IT departments to help corporate clients collect their own data. A lot has been written on the dangers of self-collecting data and the inherent risks involved when clients self-collect. Unless data is authenticated and collected in a sound forensic manner that is repeatable and defensible, then there is always the chance that it won't be admitted into evidence.

There are many examples of self-collection gone wrong, and important case law highlights these instances. When data needs to be collected, it is critically important to consider whether you should hire an outside forensic consultant. While there may be some appropriate situations which call for self-collection, I would caution legal practitioners against relying solely on clients to collect their own data.

I think the *Red Wolf* case is a perfect example of the overreliance on an IT programmer with no experience in eDiscovery. Due to his lack of experience, he wrote a flawed programming script that parsed out messages that were potentially relevant. It was exactly this type of unsuspecting error that not only caused the case to go on for almost four years, but as the judge highlighted in his opinion, is a waste of judicial resources. It even interfered with the court's ability to reduce a staggering case backlog. It's also been proven that allowing individual parties to a litigation to collect their own documents is never appropriate, particularly where they have a stake in the litigation.

Certainly, IT serves an important function for a corporation in terms of protecting their digital assets as well as the security of their systems and networks, especially while many employees are still working

in hybrid remote environments. But what they're not really looking at is the preservation of evidence. Many support functions are not trained in forensic science and may not appreciate that simply turning on a laptop or sending an e-mail could inadvertently overwrite data or cause spoliation of evidence. This type of inadvertent spoliation could quite possibly have some far-reaching consequences.

Are there certain practice areas and transactions where issues of digital forensics are more likely to arise than others?

Derek: I think the simplest application is in trade secret context, identifying unauthorized data exfiltration and proving that it occurred. I think that's the most straightforward application, but really, it is broadly applicable across all cases, because now you're trying to figure out what actually happened, across multiple systems. That expertise is applicable in analyzing the data that you have but also in figuring out what data you should be analyzing.

I call that "knowing what's knowable." AI can categorize what's in front of you, but it can't tell you that you're missing a data source that could have relevant information. That's where the expertise comes in, allowing you to say, "we want to know whether or not this particular conversation happened or if this particular information exchange occurred" between the two parties. If you just upload your e-mail and don't think broadly about how that information exchange could have happened, or ways that you can figure out whether the two parties were physically proximate to each other, you won't get the full picture.

Colleen: In my prior litigation experience, some of the biggest indicators of fraud were emails. If you look back at Enron and some of the older fraud cases, there were indicators of fraud in written communications. One of my former forensic expert colleagues used to say that when you find "call me" in an email it may be an indicator of fraud, or that the employee is a bad actor. I think we are going to see that this type of work is very important to securities litigation, really any sort of litigation, where there are allegations of fraud, embezzlement, or a Ponzi scheme.

Again, with the *Red Wolf* case, the traders were doing all of these communications through Slack. They were even brazen enough to discuss the theft of the plaintiff's trading algorithm over Slack. This is the communication we found during our forensic detective work that turned out to be the "smoking gun." The defendants were also showcasing the stolen IP in Google Vault. So, it's very interesting to see how chat messages and an eDiscovery tool for Google Workspace played an integral role.

Legal practitioners should also be on guard, because Apple just came out with a new iOS update that allows you to "undo" and "unsend" text messages. So that's going to present a new challenge for eDiscovery and digital forensics experts because you could have two bad actors at a company decide to have a conversation and then delete those emails within two minutes of receiving them. We may see more and more of this type of activity where bad actors are conspiring to make an agreement that, within a minute of each message they are sending, the other person will delete the message. To my understanding, it's still untraceable at this point. So that's only going to add a new wrinkle here for attorneys and eDiscovery professionals.

Overall, I do believe that digital forensic technology will come into play in any case where there's an implication of employee misconduct. Usually, some remnants of evidence are left behind in digital form, and if you are working with the right experts, those artifacts can be detected and uncovered. The right experts will also make important recommendations about your approach, case strategy and the best way to interpret their findings. This can make all the difference in whether you prevail in court.

In the *Red Wolf* case, the other side was only looking at the first five chat messages and the last five chat messages before and after a chat message that hit on a search term, but Derek and our team recommended a 24-hour window in which to review the chat threads. This provides a much broader context for the conversation. By adopting this approach, we were able to uncover many critical messages that were never produced, including the smoking gun. Again, if you think about it, these communications are always very informal. They're not like e-mail. And so, you want to make sure you're reconstructing the conversation in a way that actually lends context to what the individuals are talking about.

How important is it to work with a credentialed electronic data interchange (EDI) provider with in-house expertise in digital platforms in these matters?

Derek: Being from Silicon Valley, I'm not a big fan of credentials over actual knowledge. I think that staying apprised of the latest tech developments is critical. By the time something is adopted broadly enough to be a part of a credentialing system, it is already outdated. We developed our methodologies and capabilities by consciously focusing on Silicon Valley companies and their rapid rate of tool adoption.

Our client base has an adoption rate of a new tool every six months, so we had to develop methodologies that were kind of "tool-agnostic" but still figure out how to analyze data. In fact, Slack is a trend we saw coming. We wrote a paper in 2014 called "Is e-mail Dead?" and warned clients about the potential for sanctions if they didn't get a handle around how they use and manage Slack inside the enterprise.

I think it's also important to know that actors are becoming more sophisticated, and a lot of our trade secret exfiltration investigations have involved actors that were cybersecurity professionals or programmers, which is a different breed of actor. They're more adept at covering their tracks using encrypted chat – using anonymized chat or ephemeral chat that just disappears after you utilize it, but you can still find it.

Even though there are all these tools to cover your tracks, we live in the era of technological convenience, and my rule about convenience is that if it's convenient, it's tracking you. Something can only remember your preferences if it stores your preferences. And so, if it knows what restaurant you would like to go to, guess what, it knows that you've been there before, right?

On the flip side, even though there are all these great tools that can hide tracks, there's also just so much digital data

around a person that can uncover the digital truth. That's really what the UnitedLex team has been focused on. Even if we're operating outside of a system like Slack, in a broader context, we can still figure out what happened.

Colleen: I do think it's important to align with the right experts in your case. There was a reputable expert on the other side of the *Red Wolf* case, but it was our deep technological experience with Slack and exporting chat communications out of that tool that truly made the difference. This ability to analyze Slack and relay our findings in a way that everyone could comprehend was pivotal, as lead counsel noted, in securing vindication for their client.

I'm a big proponent that it's people over process and not just people over technology. We're in a very saturated market, and the way that UnitedLex differentiates ourselves in this market is really the people on our team. It is these data experts and forensic examiners that are making all the difference. While many of us in this industry can offer similar, competing technologies and innovative workflows, it's really the people behind the technology that can be the deciding factor in your case. We can all put processes and workflows in place that extract data and inform critical decisions in a case, but at the end of the day, it's all about how experienced your people are with eDiscovery and digital tools. Are they innovative? Are they creative? Are they looking at different ways of pulling the data and applying their critical judgment? You can't replicate that expertise across companies, and it can certainly determine the outcome of the case, winning or losing.

Derek: In forensics, a lot of the best tools are actually scripting tools. So you need to be a programmer and have knowledge of scripting and how to use it in order to have access to the latest techniques. A number of our forensics experts are programmers, a big reason they can figure out how to catch another programmer. They have access to all of these tools that are script-based versus relying entirely on the purchase of an expensive tool. You hit process, see what pops up, and tell the client what pops up on your initial report. But that's not the brand of forensics that we're doing at UnitedLex.

If you look at the cases we've testified on before, there are really, really deep interpretations of cloud artifact residue that other providers were not able to find. So look for those capabilities in your provider, especially if you have that type of case or you're dealing with sophisticated actors.

Colleen: Some of the experts that Derek and I were working with at UnitedLex were able to find an anomaly in the data set, and that anomaly helped us draw an inference that data may have potentially been deleted. This ability to analyze data in the right way–to understand where data lives, how data is stored, how to access that data and interpret it–is critically important.

How did your previous experience as a forensic expert help you pinpoint where to look for any potentially missing communications?

Derek: The last case, where I was actually on the other side, I had to prove that a conversation didn't happen. This was a trademark case where one party was alleging that certain relevant terms were used between the parties. And I was the expert saying that this did not happen, the opposite role as my role in the *Red Wolf* case. I had to prove a negative, and so I took a deep-dive into how that archive

was built, how it was used and then dug into the tool to show step-by-step, why nothing was there.

When you're trying to prove a negative, you need to have a very expansive, rigorous, and transparent approach. And so that's what I took. The judge in that case found our expert opinion so compelling that they awarded adverse inference instructions against the other side.

For that matter, we pointed out how we would have performed the verification had we been in their shoes. In this matter, the other party was focused on Slack export capabilities. But Slack, even though it may not be able to export a search hit, still allows you to search inside Slack. So, if you really want to know whether you accurately produced everything, you can run your own search inside.

This is also a cautionary tale for counsel: Your client is not a discovery expert who is looking at the process and saying, hey, this process makes sense.

"I think they need to know that discovery really is about determining facts right and surfacing evidence. And so playing "gotcha eDiscovery Games" is, I think, going to be really severely punished."

Colleen: To underscore Derek's point, we are talking to lawyers in the industry about more than just our digital forensics expertise. We are taking it a step further by focusing on the data science. We're starting to see even law firms now are adding data science labs and data science experts to their firms. It's been an interesting development for traditional law firms to consider how data science can create a more emotive experience for the jurors when trying cases.
There is a growing need for true data science experts, not just digital experts. Having a data science background is going to be important, because when it comes down to it, lawyers depend on experts for their critical insights. You can't manufacture that type of skill set.

In the case of - when you found the "smoking gun" exchanges - what were your first thoughts? Did you know this was the case-changing evidence as soon as you discovered it?

Derek: I don't think so. We didn't really have enough context for the case in the short amount of time, and in fact, that just shows that a good expert doesn't need full case context. We said, "this is what should have been pulled," parsed the data, and passed it to the case team. That was when they saw the smoking gun.

Colleen: I think it was a combination of things that we were looking at, not just that one message. The anomaly with the data was equally important. In fact, our team at UnitedLex was hired to replicate the workflow, to take an old Slack archive and run the search terms and come up with a production of documents from the search. After we analyzed the results for any missing messages, we also found 87 empty slack channels, which no one expected going into this. Highlighting this anomaly to the court, and suggesting that data had been deleted prior to export, was certainly a deciding factor.

When we were working on this case, we believed our findings at the time would help the attorneys and their client prevail in a second motion for sanctions. I also suspect that our findings would have factored prominently

into evidence presented to the court if the case went to trial. I don't know that we fully appreciated that the judge would actually come back and issue a default judgment, which is a rare and severe sanction for discovery abuses. And as the judge put it, he considered the totality of the circumstances when issuing his ruling. It was the repeated failure of the defendants to meet their discovery obligations and to produce relevant evidence that they were required, under law, to produce that lies at the crux of this case. Our expert findings, combined with counsel's findings concerning the deficiencies in the defendants' productions, is what helped the judge come to this determination.

One thing I do want to underscore, since this litigation dispute lasted almost four years, is that there was exceptional lawyering in the case. If the lawyers for *Red Wolf* did not continue to press, and file two motions for sanctions, then this case may have ultimately gone to trial. The judge ordered depositions to be retaken after discovery was closed, which is unusual. The legal team at Armstrong Teasdale continued to suspect that they had not received all of the relevant Slack messages and continued to petition the court concerning these deficiencies. I believe that if another legal team was less persistent, the judge may not have ordered the defendants to provide a copy of the Slack archive to the plaintiff, and our critical findings may have never been discovered.

Derek: Yes, that's where the partnering really comes in, because without their diligence, they wouldn't have received access to the data, and we would have never been able to perform our analysis.

What tips would you give practitioners just entering the realm of digital forensics? To those who want to enter the field?

Derek: Just know that it's a highly collaborative community. Digital forensics has its foundation in security and protecting people and society from bad actors. My advice is to reach out and build your expertise, build out your rigor. A lot of the best tools and knowledge are actually open source, so there's really no reason to not have deep knowledge in this area.

There is always an open invitation among digital forensics experts to reach out and talk, that's the nature of the community. And I think that's a really healthy thing, because with all of this complexity, transparency and rigor among experts is important. They're going to get us to the answer of what actually happened. There's just too much complexity for there to be gamesmanship involved in this process.

Colleen: Yes, I agree with Derek that we are part of a truly collaborative community. I would encourage anyone looking to get into the industry to reach out and connect with practitioners and discovery consulting professionals like us. There is so much opportunity right now for people just starting out: digital forensics, data science, advanced data analytics, data privacy, and even cybersecurity consulting. While there is a lot of science and computer engineering that goes into these types of positions, I also recommend sharpening your analytical and critical thinking skills. That would be a great way to round out your skill set. All in all, there is a lot of support for anyone entering the field.

Derek M. Duarte, Senior Vice President, Litigation

As a litigator and technologist, Derek brings a unique perspective to the challenges of the legal services industry. Derek has testified as an expert on eDiscovery and Computer Forensics in the state and federal courts. He gets his kicks from applying a deep understanding of digital forensics to complex litigation cases, discovering digital truth, and bad puns. He is excited by the potential of legal technology to improve access to justice, bolster our democracy and advance the practice of law. As President at BlackStone Discovery, he was named to Silicon Valley Business Journal's 40 business leaders under 40 list for driving innovation and growth in the eDiscovery industry. He is now a Senior Vice President at UnitedLex, after it acquired BlackStone Discovery.

Colleen E. Freeman, Esq., CEDS –
Senior Director, Global Litigation

Colleen has worked in the legal industry for over 20 years as a licensed attorney and a discovery consultant. She is highly sought after as a recognized expert in the field with notable experience in antitrust litigation and securities fraud. Colleen led the expert team that was chosen by the Plaintiffs' Steering Committee to support the complicated discovery work in the Blue Cross Blue Shield Antitrust Litigation. In her role as a senior director at UnitedLex, she regularly consults with Am Law 100 firms and Global Fortune 50 companies on internal investigations, complex litigation, and enforcement. She is also responsible for managing large global accounts, providing thought leadership, and building new strategic partnerships. Colleen recently held a five-year term as the President of the Association of Certified E-Discovery Specialists (ACEDS) New England Executive Board and served as a founding member of the Boston Bar Association's JD Advisory Committee.

want your eDiscovery data to work harder for you.

No problem.

We repurpose your data so you can start with a strategy, not a blank page.

Discover more at
www.unitedlex.com

UnitedLex