NO. COA12-926

NORTH CAROLINA COURT OF APPEALS

Filed: 3 September 2013

STATE OF NORTH CAROLINA

v. Wake County
No. 08 CRS 22922

BRADLEY GRAHAM COOPER

Appeal by Defendant from judgment entered 5 May 2011 by Judge Paul G. Gessner in Superior Court, Wake County. Heard in the Court of Appeals 9 April 2013.

Attorney General Roy Cooper, by Assistant Attorney General Daniel P. O'Brien and Assistant Attorney General LaToya B. Powell, for the State.

Glover & Petersen, P.A., by Ann B. Petersen, for Defendant-Appellant.

McGEE, Judge.

Bradley Graham Cooper (Defendant) and Nancy Lynn Rentz Cooper (Ms. Cooper) were married in October 2000, and they moved to Cary from Canada in January 2001. They had two daughters (the daughters). Defendant worked for Cisco Systems, Inc. (Cisco). By 2008, Defendant's marriage to Ms. Cooper was in difficulty and, by April 2008, Ms. Cooper had hired a family law attorney and planned to move out of the marital home. Defendant

and Ms. Cooper were still living in the marital home in July 2008, though they were leading mostly separate lives and were sleeping in separate bedrooms.

Defendant and Ms. Cooper attended a party at a neighbor's house on the evening of 11 July 2008. There was testimony that Defendant and Ms. Cooper argued at the party. Defendant left the party that evening, around 8:00 p.m., to put the daughters to bed. Ms. Cooper left the party a little after midnight, on 12 July 2008.

Sometime during the morning of 12 July 2008, Ms. Cooper disappeared. Defendant subsequently gave the following account of events to investigators about the morning of 12 July 2008: one of the daughters awoke between 4:00 a.m. and 4:30 a.m., and had difficulty getting back to sleep. The daughter wanted milk, but there was none at the house. Defendant went to a Harris-Teeter at about 6:30 a.m. to buy milk, and then returned home. Ms. Cooper was doing laundry, but had run out of detergent. Defendant returned to the Harris-Teeter to buy detergent and, while on his way there, received a call from Ms. Cooper asking him to get some "green juice." Receipts and surveillance video from the Harris-Teeter confirm that Defendant bought milk at 6:25 a.m., left the store, then returned and bought detergent and juice at 6:44 a.m. After Defendant bought the detergent and

juice, he returned home. At about 7:00 a.m., Ms. Cooper called to Defendant, who was upstairs, and told him she was going running. Defendant remained at home with the daughters and, when Ms. Cooper did not return from her run when expected, Defendant called a friend and cancelled a tennis date he had planned. Defendant stated he did laundry and cleaned around the house and, in the early afternoon, drove around with his daughters, looking for Ms. Cooper.

Evidence at trial tended to show that police began questioning Defendant that same day, and asked if they could take photographs of the couple's house. Defendant consented, and police photographed every room. Defendant provided police with a pair of Ms. Cooper's running shoes in order to give a police tracking dog Ms. Cooper's scent. However, the dog could not pick up a trail.

Police returned to the house the next morning, 13 July 2008, and questioned Defendant further. Police questioned Defendant more that day and the following day, 14 July 2008. Cary Police Detective George Daniels (Detective Daniels) asked Defendant for permission to look through Defendant's car and Ms. Cooper's car, and Defendant consented.

At approximately 7:00 p.m. on 14 July 2008, a body was found just off Fielding Drive, which was a short drive from

Defendant's and Ms. Cooper's house. Detective Daniels went to Defendant's house at approximately 10:00 p.m. on 14 July 2008, and informed Defendant that a woman's body had been found on Fielding Drive. At that time, identification of the body had not been determined. However, on 15 July 2008, the body was affirmatively identified from dental records as being that of Ms. Cooper. The cause of death was determined to be strangulation. The time of death could not be determined with specificity. However, it was determined that Ms. Cooper died some time in the twelve-hour period between shortly after midnight on 12 July – when she was last seen at the party – and approximately noon that same day.

Around 5:20 p.m. on 15 July, Defendant vacated his house in order to preserve the house as a possible crime scene. One of Defendant's laptops (the laptop) was left in Defendant's house and was connected to the internet for approximately twenty-seven hours on 15 and 16 July, after Defendant had vacated the house. Cary police, pursuant to a warrant, searched both Defendant's house and his car on 16 July 2008. Police also seized the laptop, along with another computer, and various other computer-related components.

Defendant was indicted for Ms. Cooper's murder on 27 October 2008. Trial began on 28 February 2011. There was

testimony concerning the strained relationship between Defendant and Ms. Cooper, and suspicious behavior on the part of Defendant, both before and after Ms. Cooper's disappearance. However, the sole direct evidence linking Defendant to the murder was obtained from the laptop that had been left on and connected to the internet after Defendant vacated his house.

The State presented expert testimony from FBI Special Agent Greg Johnson (Special Agent Johnson) and Durham Police Detective Chris Chappell (Detective Chappell), both of whom testified as forensic computer analysts. Special Agent Johnson and Detective Chappell were forensic examiners of the Computer Analysis Response Team (CART). CART extracts "evidence off of seized digital media" such as computer hard drives. The first part of the forensic process involves taking inventory of the components. CART then checks for any portable media in or attached to the computer, opens up the case of the CPU and removes the hard drive(s). CART handles all seized material carefully so as not to compromise or contaminate the data. According to Special Agent Johnson's testimony, the integrity of the hard drive is protected by making a "forensic image" of the drive, which is "a copy that we make of the hard drive. It's a bit-per-bit copy, which gets every piece of . . . information off of the hard drive and puts it into what we call forensic

image." Examination then occurs of a different hard drive containing the forensic image, not the original hard drive. The forensic image requires some type of specialized software to read and "interpret those files that it creates."

Members of the CART team performed these forensic retrieval and information processing techniques on the hard drive from the laptop. The CART team used software called Forensic Tool Kit, or FTK, to process that hard drive. FTK and similar programs index files retrieved from the hard drive, allowing for specific searches for particular data to be performed. An FTK report was then created based upon the particular search parameters utilized. One of the sub-sets of files collected in the FTK report for Defendant's laptop was temporary internet history files for dates close in time to Ms. Cooper's murder.

Special Agent Johnson and Detective Chappell testified that the temporary internet files recovered from the laptop indicated someone conducted a Google Map search on the laptop at approximately 1:15 p.m. on 11 July, the day before Ms. Cooper was murdered. They concluded that this search was done by someone using the laptop while it was at the Cisco office where Defendant worked. The State's experts testified that the Google Map search was initiated by someone who entered the zip code associated with Defendant's house, and then moved the map and

zoomed in on the exact spot on Fielding Drive where Ms. Cooper's body was found.

Defendant presented evidence at trial. Defendant called Jay Ward (Ward) to testify concerning the incriminating Google Map files recovered from the laptop. Ward had worked for more than fifteen years in the computer field, specializing in computer network security. When Defendant called Ward, the State objected, challenging Ward's credentials to testify as an expert concerning the relevant Google Map files.

The State focused on Ward's lack of training and experience as a forensic computer analyst. The trial court agreed with the State and, on 19 April 2011, ruled that Ward could not testify specifically about the Google Map files. Ward was allowed to give general testimony concerning the ease with which files could be altered or planted on a computer that, like Defendant's, had been left connected to the internet. Defendant argued, since the trial court did not find the methods by which Ward obtained his data to be reliable, that Ward be allowed to testify based upon the data produced by the State's forensic analysts. The trial court denied Defendant's request. Ward testified on *voir dire* that had he been allowed to, he would have offered his opinion that the incriminating Google Map files had been planted on Defendant's computer, and he would have

further testified to the specific aspects of the files that had led him to this conclusion.

Following the trial court's ruling, Defendant immediately sought a forensic computer analyst that he could call to testify concerning the Google Map files. Defendant located a forensic computer analyst, Giovanni Masucci (Masucci), on 20 April 2011. As the court session began on 21 April 2011, Defendant gave notice of Masucci as Defendant's replacement expert. Masucci had examined the data produced by the State's forensic computer analysts, and produced a report. Masucci's report indicated that the data results obtained by Ward matched the results obtained by CART. Masucci's conclusion was the same as Ward's: that the Google Map files had "been placed on the hard drive [and] could not have been the result of normal internet activity." Masucci's *curriculum vitae* was sent to the State on 22 April 2011, and Masucci's report was sent the next day. Court was not in session on these days.

Court resumed on 25 April 2011, and Defendant attempted to call Masucci. The State objected on the basis that Masucci was not on the list of experts Defendant provided to the State before trial, nor had the State been provided with Masucci's report prior to trial, and these failures constituted discovery rules violations. The trial court again agreed with the State,

and ruled that Defendant had violated the discovery statutes by failing to notify the State that he was planning to call Masucci, and by failing to provide Masucci's *curriculum vitae* and report prior to the beginning of the trial. As a sanction for the discovery violations found by the trial court, the trial court ruled that Masucci could not testify. Pursuant to North Carolina Rule of Evidence 403, the trial court also ruled that allowing Masucci to testify would prejudice the State, and that this prejudice would substantially outweigh any probative value of Masucci's testimony. Defendant was prohibited from calling any witness to testify that the actual Google map files relied upon by the State to connect Defendant to the site where Ms. Cooper's body was found were corrupt or had been tampered with in any manner.

The jury returned a verdict of guilty of first-degree murder on 5 May 2011. Defendant was sentenced to life in prison without the possibility of parole. Defendant appeals.

I. Issues

Defendant brings forward three arguments on appeal: (1) whether the trial court erred in precluding the testimony of Masucci as a sanction for discovery rules violations, (2) whether the trial court erred in limiting Ward's testimony and preventing Ward from testifying that, in his opinion, the Google

Map files had been planted on the laptop and, (3) whether the trial court erred in denying Defendant's motion to compel certain discovery. We address Defendant's second argument first.

II. Ward's Testimony

In Defendant's second argument, he contends that "the trial court's ruling that . . . Ward was not qualified to give expert testimony about tampering on [Defendant's] computer was an abuse of discretion and deprived Defendant . . . of his state and federal constitutional due process right to present a defense." We agree.

It is well settled that "appellate courts must 'avoid constitutional questions, even if properly presented, where a case may be resolved on other grounds.'" *James v. Bartlett*, 359 N.C. 260, 266, 607 S.E.2d 638, 642 (2005) (citation omitted). Generally, the decision of a trial court to exclude expert witness testimony is reviewed for an abuse of discretion. *Howerton v. Arai Helmet, Ltd.*, 358 N.C. 440, 458, 597 S.E.2d 674, 686 (2004) (citation omitted). However, "'[c]onstitutional rights are not to be granted or withheld in the court's discretion.'" *State v. Vereen*, 312 N.C. 499, 508, 324 S.E.2d 250, 256 (1985) (citations omitted).

> The question presented here is one of law rather than discretion, for "(t)he right to

> . . . face one's accusers and witnesses with other testimony (is) guaranteed by the Sixth Amendment to the Federal Constitution which is made applicable to the States by the Fourteenth Amendment, and by Article I, Sections 19 and 23 of the Constitution of North Carolina."

State v. Brower, 289 N.C. 644, 660, 224 S.E.2d 551, 562 (1976) (citation omitted); *see also*, *State v. Mason*, 295 N.C. 584, 589, 248 S.E.2d 241, 245 (1978); *State v. Farrell*, 223 N.C. 321, 326-27, 26 S.E.2d 322, 325 (1943); *State v. Banks*, 210 N.C. App. 30, 47, 706 S.E.2d 807, 820 (2011) (citation omitted).

We note that the cases cited above concern denials of motions to continue. However, if the denial of a right to present a witness constitutes error, we are unable to distinguish between the constitutional significance of the denial of a defendant's right to present a witness through denial of a continuance, and the denial of a defendant's right to present a witness through a misapplication of a rule of evidence. *See Fry v. Pliler*, 551 U.S. 112, 121-22, 168 L. Ed. 2d 16, 23-4 (2007); *Holmes v. South Carolina*, 547 U.S. 319, 324-31, 164 L. Ed. 2d 503, 508-13 (2006); *Montana v. Egelhoff*, 518 U.S. 37, 52-53, 135 L. Ed. 2d 361, 373-74 (1996) (plurality opinion); *Green v. Georgia*, 442 U.S. 95, 99, 60 L. Ed. 2d 738, 742 (1979); *Chambers v. Mississippi*, 410 U.S. 284, 298-303, 35 L. Ed. 2d 297, 310-13 (1973). Of course, there can only be a

constitutional violation if the evidence is excluded for an invalid reason. *Holmes*, 547 U.S. at 324-31, 164 L. Ed. 2d at 508-13.

Accuracy in criminal proceedings is a particularly compelling public policy concern:

> The private interest in the accuracy of a criminal proceeding that places an individual's life or liberty at risk is almost uniquely compelling. Indeed, the host of safeguards fashioned by this Court over the years to diminish the risk of erroneous conviction stands as a testament to that concern. The interest of the individual in the outcome of the State's effort to overcome the presumption of innocence is obvious and weighs heavily in our analysis.

Ake v. Oklahoma, 470 U.S. 68, 78, 84 L. Ed. 2d 53, 63 (1985). The United States Supreme Court has stated that a defendant on trial has a greater interest in presenting expert testimony in his favor than the State has in preventing such testimony:

> The State's interest in prevailing at trial - unlike that of a private litigant – is necessarily tempered by its interest in the fair and accurate adjudication of criminal cases. Thus, also unlike a private litigant, a State may not legitimately assert an interest in maintenance of a strategic advantage over the defense, if the result of that advantage is to cast a pall on the accuracy of the verdict obtained. We therefore conclude that the governmental interest in denying [the defendant] the assistance of [an expert witness] is not substantial, in light of the compelling interest of both the State and the

> individual in accurate dispositions.

Ake, 470 U.S. at 79, 84 L. Ed. 2d at 63-64. Nonetheless, trial courts are granted substantial freedom to regulate conduct and evidence at trial:

> We acknowledge also our traditional reluctance to impose constitutional constraints on ordinary evidentiary rulings by state trial courts. In any given criminal case the trial judge is called upon to make dozens, sometimes hundreds, of decisions concerning the admissibility of evidence. As we reaffirmed earlier this Term, the Constitution leaves to the judges who must make these decisions "wide latitude" to exclude evidence that is "repetitive . . ., only marginally relevant" or poses an undue risk of "harassment, prejudice, (or) confusion of the issues." Moreover, we have never questioned the power of States to exclude evidence through the application of evidentiary rules that themselves serve the interests of fairness and reliability – even if the defendant would prefer to see that evidence admitted.

Crane v. Kentucky, 476 U.S. 683, 689-90, 90 L. Ed. 2d 636, 644 (1986) (citations omitted). In *Crane*, the United States Supreme Court discussed the impact on a defendant's trial of the exclusion of evidence favorable to the defendant bearing on a central issue in the trial:

> [W]ithout "signal(ing) any diminution in the respect traditionally accorded to the States in the establishment and implementation of their own criminal trial rules and procedures," we have little trouble concluding on the facts of this case that the blanket exclusion of the proffered

> testimony about the circumstances of petitioner's confession deprived him of a fair trial.
>
> Whether rooted directly in the Due Process Clause of the Fourteenth Amendment, or in the Compulsory Process or Confrontation Clauses of the Sixth Amendment, the Constitution guarantees criminal defendants "a meaningful opportunity to present a complete defense." We break no new ground in observing that an essential component of procedural fairness is an opportunity to be heard. That opportunity would be an empty one if the State were permitted to exclude competent, reliable evidence bearing on the credibility of a confession when such evidence is central to the defendant's claim of innocence. In the absence of any valid state justification, exclusion of this kind of exculpatory evidence deprives a defendant of the basic right to have the prosecutor's case encounter and "survive the crucible of meaningful adversarial testing."

Id. at 690, 90 L. Ed. 2d at 645 (citations omitted). Though the above citations involve constitutional questions, they also inform our analysis of whether there was an abuse of discretion in preventing Ward from giving his opinion that the Google Map files from Defendant's laptop had been tampered with.

Rule 702

A.

The admissibility of expert testimony is controlled by Rule 702 of the North Carolina Rules of Evidence:[1]

[1] Rule 702 was amended by S.L. 2011-283, § 1.3. However, these changes only apply to actions commenced on or after 1 October

> "If scientific, technical or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education may testify thereto in the form of an opinion." N.C. Gen. Stat. § 8C-1, Rule 702(a) (2004). "It is well-established that trial courts must decide preliminary questions concerning . . . the admissibility of expert testimony." *Howerton v. Arai Helmet, Ltd.*, 358 N.C. 440, 458, 597 S.E.2d 674, 686 (2004). . . . .
>
> *Howerton* sets forth a three-step test for determining the admissibility of expert testimony: "(1) Is the expert's proffered method of proof sufficiently reliable as an area for expert testimony? (2) Is the witness testifying at trial qualified as an expert in that area of testimony? (3) Is the expert's testimony relevant?" . . . .
>
> "'The essential question in determining the admissibility of opinion evidence is whether the witness, through study and experience, has acquired such skill that he is better qualified than the jury to form an opinion as to the subject matter to which his testimony applies.'"

Miller v. Forsyth Mem'l Hosp., Inc., 173 N.C. App. 385, 389, 618 S.E.2d 838, 841-42, *on reh'g*, 174 N.C. App. 619, 625 S.E.2d 115 (2005) (some citations omitted). "[W]e discern no qualitative difference between credentials based on formal, academic training and those acquired through practical experience." *Howerton*, 358 N.C. at 462, 597 S.E.2d at 688. In *Howerton*, our

---

2011.

Supreme Court expressly rejected the adoption of the federal standard for assessing the foundational reliability of expert testimony as set forth in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 125 L. Ed. 2d 469 (1993). *Howerton*, 358 N.C. at 469, 597 S.E.2d at 693. In rejecting the *Daubert* approach, our Supreme Court stated:

> One of the most troublesome aspects of the *Daubert* "gatekeeping" approach is that it places trial courts in the onerous and impractical position of passing judgment on the substantive merits of the scientific or technical theories undergirding an expert's opinion. We have great confidence in the skillfulness of the trial courts of this State. However, we are unwilling to impose upon them an obligation to expend the human resources required to delve into complex scientific and technical issues at the level of understanding necessary to generate with any meaningfulness the conclusions required under *Daubert*.

Id. at 464-65, 597 S.E.2d at 690. "'[F]ew judges possess the academic credentials or the necessary experience and training in scientific disciplines to separate competently high quality, intricate scientific research from research that is flawed[.]'" *Id.* at 466, 597 S.E.2d at 691 (citation omitted). Our Supreme Court cited a critic of *Daubert*, who opined that the "post-*Daubert* era can fairly be described as the period of 'strict scrutiny' of science by non-scientifically trained judges[,]" *Id.* at 466, 597 S.E.2d at 691 (citation omitted); *see also id.*

at 460-61, 597 S.E.2d at 687-88. "[A]pplication of the North Carolina approach is decidedly less mechanistic and rigorous than the 'exacting standards of reliability' demanded by the federal approach." *Id.* at 464, 597 S.E.2d at 690. "'[V]igorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence.'" *Id.* at 461, 597 S.E.2d at 688 (citation omitted); *see also*, *Crocker v. Roethling*, 363 N.C. 140, 675 S.E.2d 625 (2009).

The United States Supreme Court has also stated that the right of a defendant to present witnesses in the defendant's defense is fundamental:

> Few rights are more fundamental than that of an accused to present witnesses in his own defense[.] Indeed, this right is an essential attribute of the adversary system itself.
>
> > "We have elected to employ an adversary system of criminal justice in which the parties contest all issues before a court of law. The need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. The very integrity of the judicial system and public confidence in

> the system depend on full disclosure of all the facts, within the framework of the rules of evidence. . . ."

The right to compel a witness' presence in the courtroom could not protect the integrity of the adversary process if it did not embrace the right to have the witness' testimony heard by the trier of fact. The right to offer testimony is thus grounded in the Sixth Amendment even though it is not expressly described in so many words:

> "The right to offer the testimony of witnesses . . . is in plain terms the right to present a defense, the right to present the defendant's version of the facts as well as the prosecution's to the jury so it may decide where the truth lies. Just as an accused has the right to confront the prosecution's witnesses for the purpose of challenging their testimony, he has the right to present his own witnesses to establish a defense. This right is a fundamental element of due process of law."

Taylor v. Illinois, 484 U.S. 400, 408-09, 98 L. Ed. 2d 798, 810 (1988) (citations omitted); *see also Rock v. Arkansas*, 483 U.S. 44, 54-55, 97 L. Ed. 2d 37, 48-9 (1987). With these principles in mind, we must evaluate evidence regarding Ward's experience and credentials to determine if the trial court erred in excluding Ward's opinion testimony that the Google Map files located on the laptop had been tampered with.

B.

After the State concluded presentation of its evidence, it moved *in limine* to exclude Ward from testifying. Defendant objected:

> [Defendant's counsel]: And, Your Honor, we -- we would certainly object at this time to a motion in limine, given the fact that the State has had Mr. Ward on the witness list as a potential expert for quite some time now, with no -- no notice as to the concept that they were going to be moving in limine to exclude his testimony. If that was the route that they were seeking to take, that should have occurred at a more appropriate time. I certainly understand, if he wants to take Mr. Ward on voir dire, that that is appropriate.

The trial court denied Defendant's objection, and Ward testified on *voir dire* as indicated below.

Ward testified on *voir dire* that his interest in computers began in 1982, and that he was first hired as a network administrator by a Research Triangle Park company called Persimmon Information Technologies in approximately June 1997. This job included "ensuring that all of the firewall rules were correct[,]" which broadly meant keeping "unintended people out" of the computer system, which consisted of a few hundred computers. Most of the security issues Ward addressed during this time were "intrusion attempts from the internet." In order to determine where those intrusions came from, Ward examined log

files and the timestamps on the log files to "create a time line to find out exactly what's going on."

In November 1998, Ward began working for Carolinas Healthcare in Charlotte as its "senior security analyst, or senior firewall administrator[.]" The bulk of Ward's work consisted of reviewing computer log files, because "[t]hat's where you find most of the activity on the network." Ward worked on projects to insure the safe movement of private medical data between the member practices and institutions of Carolinas Healthcare. Identifying "intrusion" into the system was one of Ward's job duties. Ward was working with thousands of systems, and described some of his duties and concerns as follows:

> Well, it's -- it's not just [knowing] computer operating systems as required. It's a -- a plethora of things, from understanding the communications path of how packets move across the internet, so there's a networking aspect to it. There's also a -- a component for the system -- the actual host or the actual server, what's going on, understanding how the various ports that are open on a machine might be used either for good or maliciously, which kind of goes into the field of understanding how viruses work, or Trojans work and the types of things that they are trying to attempt to access on a computer. Also, too, how things are written to logs in the event for logons, for processes that are actually functioning or being triggered on the machine, and if any of the -- the files have been changed.

> So, and -- and towards that vein, one of the things that we would -- we would typically use, but you don't find it much any more, is a program called Tripwire. And Tripwire is used for integrity of files. So basically you run a script against all of your files once you have a production-ready level server, and it will actually do hashes of all of the files on the system, put them off to a side and then, in the event that any of those files change, you -- you then have a -- a potential way to go back and say, okay, this file was changed; we need to reinstall the correct version in the event of any sort of penetration.

In 1999, Ward began working for First Citizens Bank as a senior security engineer. Ward testified that his two biggest projects at First Citizens were ensuring "the security of the internet pipe," and developing "the ability for First Citizens to take [its] online banking platforms, move them from the third party and move them in-house, so that we had complete control over them." Part of this involved "architecting the security infrastructure," and "ensuring that security, not only at the perimeter via firewalls and via intrusion detection was in place, but also that host intrusion detection or intrusion prevention was in place." Ward estimated that his computer security services for First Citizens bank were helping to protect between five and seven billion dollars in assets. Ward's work at First Citizens included both the network system

as a whole and individual computer work station security. Ward testified:

> As . . . part and parcel of reviewing the logs - well, you'll often see things [in the files] that are just - that don't look right or track patterns don't look right[.]. . . And in so doing, I would often find potential -- or intrusion attempts that were basically knocking on the door on the outside of the firewall.

Ward was also responsible for investigating suspicious activity of employees, including investigating employees' internet histories.

Ward testified that he used specialized software programs, such as EnCase and FTK, to assist in sorting through file data, but that there were limitations in using the software alone:

> I think that Agent Johnson or any other FBI worth their salt will tell you that it's not just tools that are important, but what you look at and understanding how -- how things look in any sort of log files and to give you, not necessarily a hunch, but things that don't look right, based upon experience of having done it for so long.
>
> So typically -- typically, whenever you see something like an internet port scan or something like that, they're automated tools -- right? -- that anybody can run. Just click a little button and it will go out and it will look for the -- the low-hanging fruit, if you will. Seeing those types of things in logs is generally a good first indication that something is amiss, or that someone is doing recognizance work against your network.

Q. Now, . . . when looking for people's internet activity or towards a potential theft, did the time of the conduct ever become an issue in your investigations?

A. It did. . . . .

. . . .

Q. When performing that task and attempting to evaluate the time of activity, would you rely solely on a tool like EnCase or FTK?

A. Absolutely not.

Q. And why not?

A. Well, there's -- there's several reasons. Don't get me wrong, those types of tools are great for things that may have happened on an individual machine; however, there are some shortcomings of any software program. They're in general only as good as the people that -- that write them or the -- the specs that people have asked them to write them to. It wouldn't necessarily capture all of the information that may have been traversing the network.

Additionally, as I say, the reports that are generated from these types of forensic tools are generally -- are generally good, as -- as an overall statement, in providing you with vast amounts of information. And -- and, specifically in this case, I think that there were 170 something thousand files to look through, which is -- which is fine; however, trying to pinpoint something in those files and knowing exactly -- or being able to research and find out what the individual files are becomes a little more problematic.

And these tools don't necessarily go to that level, so it's -- it's based upon experience

> in having gone through some of these types of things before that -- it's important to look into the actual files, especially within a specific time frame that the alleged activity was supposed to have occurred.
>
> Q. Are you familiar with the terms "file name attributes" and "system information attributes"?
>
> A. I am.
>
> Q. And are you aware if the tools EnCase and FTK are even capable of evaluating file name attribute?
>
> A. They are not. Not only that, but FTK is actually not capable of noticing any file modifications or signature modifications on a file. So, if you were to change like a -- a file extension, or something like that, it's not going to pick that up.

Ward began working as an "information security architect" for Cisco Systems in 2002. Ward testified that he had many duties at Cisco, and described one such duty as follows:

> I was on the team for the implementation for Cisco's public key infrastructure. Now, I realize you might not know what that means, so suffice it to say that it -- it involves a -- a high understanding of cryptography, of encryption and decryption as it pertains to certificates. So -- and -- and I'll give you a really good example. A certificate that, when you go to a website and you go to a secure website and it brings up the certificate, you've probably never looked at it; most people don't. But those types of things have a -- a trust chain, so -- and they're all mathematically linked by virtue

of a public key infrastructure.

In approximately 2005, Ward began working for Symantec, then known as "@stake." Ward described Symantec as a "white hat hacking company[.]" Symantec

> was hired by Fortune 500, Fortune 1000 companies, municipalities, governments, states to do penetration testing exercises. And that could be from the mobility side, which would be wireless, from web application, from external network penetration, to internal network penetration, to check for vulnerabilities internally, as social engineering, and obviously pretending to be someone that you're not in order to infiltrate some place else.

Ward's job was "[k]eeping people out of assets that they are not supposed to be in." Ward testified that he had conducted "hundreds" of these tests. Ward further testified that part of his job was looking at the file logs on particular computers to determine if there had been an intrusion and, if so, "what had happened." Part of this process was using forensic tools, including FTK, EnCase, and others.

In 2007, Ward left Symantec to form his own computer system security company, WireGhost Security, Inc. (WireGhost), a Raleigh-based computer network security company. At the time of trial, Ward was still the owner of WireGhost. Ward described his business as: "Penetration testing, risk assessments, . . . host hardening, understanding the internals

of computers." When asked on *voir dire* if his business was to protect computers "from somebody getting into" the computers, he answered in the affirmative.

Ward testified that he was a Certified Information Systems Security Professional, a Cisco-certified network professional, and also had multiple firewall certifications. Ward was a member of InfraGard, "the public and private joint partnership between security professionals and . . . the Federal Bureau of Investigation[,]" and served as its vice-president from 2003 to 2005. Ward had also published multiple articles in the field of data security.

On cross-examination, Ward testified that his resume did not include anything specifically concerning "forensic examinations of computers" and that his expertise was primarily "in the field of network security[.]" Ward testified that he had only done two forensic examinations, involving approximately nine computers. Ward testified that he did not hold a certification for the EnCase software he used to conduct the forensic examinations in those two instances. The State asked Ward: "And then you're asked to investigate – forensically investigate the computers in this case; is that accurate?" Ward responded: "I was asked to look at the analysis as provided by the FBI for this case." When asked if he was an expert in

forensics, Ward replied: "No, sir. But you don't have to be to analyze the data." The following colloquy occurred between Defendant's attorney and Ward:

> Q. [Y]ou've spoken about specifically doing forensics on machines.
>
> A. Correct.
>
> Q. The remainder of your job as a . . . senior security analyst for the last 18 years, has that involved researching specific incidents on machines, finding out the cause, and looking into exactly what happened at set instances in time?
>
> A. Yes, sir.
>
> . . . .
>
> Q. When you say that you'd only done [two computer forensic analyses] . . . you're not including in that all of the separate instances as a security analyst . . . where you've looked at individual work stations to evaluate whether there was tampering present on those work stations[.]
>
> A. [C]orrect.

Ward then testified that the number of individual work stations he had evaluated in his career "to determine whether or not there was tampering" was "in the hundreds." Ward also testified that it was "standard operating procedure" to investigate the internet history of computers he examined to determine, as Defendant's attorney put it, "what happened at what time[.]" Ward testified that normally, "every single time

I'm asked to look at a computer[,]" one of the places he [would] check was "the temporary internet files."

> Q. And what was it that you were asked to verify in this particular case?
>
> A. That tampering possibly could have occurred.
>
> Q. With what type of files?
>
> A. With Google Map files.
>
> Q. And are those temporary internet files?
>
> A. Indeed they are, sir.
>
> Q. And that's the type of exam you've done hundreds of times?
>
> A. Yes.

While admitting that he was not formally trained or certified on any forensic tools, Ward testified that he did not think that was important because "the only thing I was trying to do [was] [replicate] what the FBI had done so that I was looking at . . . the same type of . . . data." Ward testified that when he conducted those tests and extracted that data, the defense had not yet been provided with the data recovered by the FBI using FTK or any other forensic tools. Ward testified that, later, after comparing what he retrieved with what was retrieved by the FBI, he would know if the data he obtained matched the FBI data. On 18 April 2011, Ward was asked when he was "first given opportunity to even look at the FBI's version of the

master file tables?" Ward responded: "It was late last week when they gave -- gave us a copy of the CD-Rom." There was testimony by the State's witnesses suggesting that the Google Map file data recovered by Ward was substantially similar to that recovered by the FBI.

C.

Following *voir dire*, Defendant's counsel argued that Ward should be qualified as an expert because his "knowledge, skill, experience, training, [and] education" better qualified him, rather than the jury, to make determinations concerning the files recovered from Defendant's hard drive. Defendant's counsel argued:

> I believe that [Ward] qualifies in every possible respect as an expert, that the data extraction itself is actually irrelevant to this testimony, as the - the exact same conclusions that Mr. Ward draws from his own data, can be drawn simply from the FBI's data.
>
> As we have heard from testimony, Officer Chappell testified that the MFT [(master file table)] that we have provided was substantially similar to the one that they had provided. And, in fact, went on to compare the error rates in timestamps between the two, but never actually attacked the validity of the data that we had provided in our own MFT, and had an opportunity to do that.
>
> Now, I - I don't think there is any question but that Mr. Ward is the appropriate and qualified witness.

The State attacked Ward's experience as a "forensic examiner," highlighting Ward's testimony that he was not certified on the forensic tools he used to extract his data, that he had not performed many forensic examinations in the past, that he had never testified as an expert, that there was no way for the State to replicate the tests Ward performed, and that Ward testified that he did not consider himself an "expert" in forensic computer analysis. Defendant's counsel argued that, if the State did not trust Ward's techniques for data extraction, Ward could testify using the FBI data:

> [Defendant's counsel]: We could switch out all of the data that [the State's] talking about, and Mr. Ward can give the exact same opinion based on the data that the FBI has provided. Since whether or not Mr. Ward recalls, or whether or not [the State] is going to state it, the data's the same with the exception of the last -- with the exception of millionths of a second. They have the same number of invalid timestamps. We can simply accept that data, if [the State] has some question as to the extraction techniques.
>
> But moreover, what [the State] is not addressing is that there is a hierarchy of expertise in computers, and there are people that are able to do lower-level tasks, such as working with programs, pushing buttons, making things like forensic tool kit churn out a result. And, as you go up the hierarchy, the people who are at the pinnacle are actually those who are capable of network and system administration, and who are capable of detecting that kind of

> intrusion and tampering. That is actually the same kind of training that Special Agent Johnson had, with respect to intrusion. We go to Officer Chappell, on the other hand, he had looked at, I believe, five computers prior to this case.
>
> So the idea that [the State] is attempting to impeach Mr. Ward's capabilities, I -- given his wealth of experience, and specifically his wealth of experience in identifying tampering, is absurd. And I believe that this is entirely within the jury's province.

The trial court asked Defendant if Ward's testimony concerning the FBI data would be "as a forensic examiner." Defendant's counsel answered, "No, sir. That's his opinion as a computer security professional that tampering occurred. Determination as to whether something has been penetrated, and as to whether something has been tampered with, is directly within the province of a computer security professional, and that is exactly what Mr. Ward is."

The trial court ruled that Ward could testify as "an expert witness in the field of network security and vulnerability assessment[,]" but not as an expert "forensic examiner[.]" The trial court was troubled that there were "a number of the reports and tests that - that being specifically the Helix test that's not in [Ward's] report, and that he was supervised and told what to do by someone else [when using some of the forensic software]."

When asked by Defendant's counsel if the trial court's ruling prevented Ward from testifying about the FBI data, the trial court stated, "he is not qualified to interpret their data because that data was admitted as a forensic analysis or analyst data, and that's – that would basically be allowing him to testify as a forensic analyst, by taking their data and . . . testifying from it." The trial court stated that its ruling was based primarily on *State v. Ward*, 364 N.C. 133, 694 S.E.2d 738 (2010). The trial court then also excluded Ward's testimony, based upon Rule 403 of the North Carolina Rules of Evidence, ruling that the probative value of the evidence to Defendant was substantially outweighed by the prejudicial effect of that evidence to the State.

D.

Even if we assume, without deciding, that the trial court did not err in excluding Ward from testifying as an expert in forensic computer analysis, the trial court did err in limiting Ward's testimony in such a manner that prevented him from testifying concerning data retrieved from the laptop, including the Google Map files.

The bulk of the *voir dire*, and the arguments by the State in favor of excluding Ward's testimony, centered on Ward's experience in forensic data retrieval. According to the

testimony of Special Agent Johnson and Detective Chappell, forensic data retrieval included: securing and removing a hard drive, protecting the hard drive from further alteration, creating forensic copies of the hard drive to use for analysis, and then using specialized software to retrieve and catalog digital data from the forensic copy of the hard drive. The State did not seriously challenge Ward's ability to understand and interpret the actual data retrieved, and the *voir dire* testimony indicated that Ward had been examining precisely the kind of files at issue – temporary internet files – on a regular basis throughout his long career as a digital data security professional.

> It is not necessary that an expert be experienced with the identical subject matter at issue or be a specialist, licensed, or even engaged in a specific profession. It is enough that the expert witness "because of his expertise is in a better position to have an opinion on the subject than is the trier of fact."

State v. Morgan, 359 N.C. 131, 160, 604 S.E.2d 886, 904 (2004) (citation omitted). According to his *voir dire* testimony, Ward *was engaged* in a specific profession in the type of analysis in which the defense wanted him to testify, and *was experienced* with the identical subject matter – temporary internet files –

at issue. Ward was certainly "in a better position to have an opinion on the subject than [wa]s the trier of fact." *Id*.

The trial court apparently believed that, because the digital data was recovered using forensic tools and methods, only an expert forensic computer analyst was qualified to interpret and form opinions based on the data recovered. The evidence on *voir dire* does not support this understanding of the nature of Ward's expertise. Assuming *arguendo* that the data Ward recovered from the forensic copy of the hard drive was suspect, neither the State nor Defendant argued that the data recovered by the State's experts was flawed – just that there was disagreement concerning the interpretation of that data. Nothing in evidence supports a finding that Ward was not qualified to testify using the data recovered by the State. Ward, based upon expertise "acquired through practical experience," *Howerton*, 358 N.C. at 462, 597 S.E.2d at 688, was certainly "better qualified than the jury to form an opinion as to the subject matter to which his testimony applie[d]." *Miller*, 173 N.C. App. at 389, 618 S.E.2d at 841-42; *see also*, generally, *State v. Ward*, 364 N.C. 133, 694 S.E.2d 738 (2010); *Crocker v. Roethling*, 363 N.C. 140, 675 S.E.2d 625 (2009).

We cannot find sufficient evidence in the record to support the trial court's exclusion of Ward's testimony, as indicated

above, for any of the three prongs of the *Howerton* analysis. *Howerton*, 358 N.C. at 458, 597 S.E.2d at 686. The Google Map files recovered from Defendant's laptop were perhaps the most important pieces of evidence admitted in this trial. We hold that the trial court abused its discretion in excluding Ward from testifying, relying on the State's own evidence, to his opinion that the Google Map files recovered from Defendant's laptop had been tampered with.

Assuming *arguendo* the trial court did not abuse its discretion in disallowing Ward from giving his opinion concerning the Google Map files, *James*, 359 N.C. at 266, 607 S.E.2d at 642, we hold that the trial court erred in violation of the constitutions of the United States and North Carolina. *Farrell*, 223 N.C. at 326-27, 26 S.E.2d at 325.

Rule 403

The trial court also excluded Ward's testimony pursuant to Rule 403 of the North Carolina Rules of Evidence. Rule 403 states: "Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence." N.C.R. Evid. Rule 403 (2011). "Whether or not to exclude evidence under Rule

403 of the Rules of Evidence is a matter within the sound discretion of the trial court and its decision will not be disturbed on appeal absent a showing of an abuse of discretion." *State v. McCray*, 342 N.C. 123, 131, 463 S.E.2d 176, 181 (1995) (citation omitted). However,

> [t]he question presented here is one of law rather than discretion, for "(t)he right to . . . face one's accusers and witnesses with other testimony (is) guaranteed by the Sixth Amendment to the Federal Constitution which is made applicable to the States by the Fourteenth Amendment, and by Article I, Sections 19 and 23 of the Constitution of North Carolina."

Brower, 289 N.C. at 660, 224 S.E.2d at 562 (citations omitted).

The probative value of the testimony excluded was not "outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence." N.C.R. Evid. Rule 403. We hold that the exclusion of Ward's testimony constituted an abuse of discretion pursuant to general Rule 403 analysis.

Prejudice

The sole physical evidence linking Defendant to Ms. Cooper's murder was the alleged Google Map search, conducted on Defendant's laptop, of the exact area where Ms. Cooper's body was discovered. Absent this evidence, the evidence connecting

Defendant to this crime was primarily potential motive, opportunity, and testimony of suspicious behavior. We hold, whether the error was constitutional or not, that erroneously preventing Defendant from presenting expert testimony, challenging arguably the strongest piece of the State's evidence, constituted reversible error and requires a new trial, because "there is a reasonable possibility that, had the error in question not been committed, a different result would have been reached at the trial out of which the appeal arises." N.C. Gen. Stat. § 15A-1443(a) (2011); *see also Taylor*, 484 U.S. at 409, 98 L. Ed. 2d at 810-11; *State v. Moore*, 321 N.C. 327, 344-47, 364 S.E.2d 648, 656-58 (1988). Assuming constitutional analysis applies, we also hold that the State has failed to show that the error was "harmless beyond a reasonable doubt." N.C.G.S. § 15A-1443(b).

III.

In Defendant's first argument, he contends that the trial court erred in precluding the testimony of Masucci, a forensic computer analyst, 'as a sanction for purported discovery violations[.]" We agree.

In light of our holding above, and because this issue is not likely to recur, we are not required to address this argument. However, resolution of this issue presents an

alternate basis for granting a new trial. Therefore, in an abundance of caution, we address it.

The State did not indicate before trial that it intended to challenge Ward. Defendant called Ward, intending for Ward to testify, based upon his analysis of the data recovered from Defendant's laptop, that the Google Map files had been tampered with. The State successfully moved to exclude this testimony on the basis that Ward was not an expert in computer forensic analysis. Defendant quickly located Masucci, an expert in computer forensic analysis, to provide the testimony Ward was prevented from giving. The State then moved to exclude Masucci as a sanction for violation of discovery rules.

Based upon the facts in this case, Defendant was required under N.C. Gen. Stat. § 15A-905 (2011) to:

> Give notice to the State of any expert witnesses that the defendant reasonably expects to call as a witness at trial. Each such witness shall prepare, and the defendant shall furnish to the State, a report of the results of the examinations or tests conducted by the expert. The defendant shall also furnish to the State the expert's curriculum vitae, the expert's opinion, and the underlying basis for that opinion. The defendant shall give the notice and furnish the materials required by this subdivision within a reasonable time prior to trial, as specified by the court.

Generally, "[w]hether a party has complied with discovery and what sanctions, if any, should be imposed are questions

addressed to the sound discretion of the trial court." *State v. Tucker*, 329 N.C. 709, 716, 407 S.E.2d 805, 810 (1991) (citation omitted). A trial court may grant a continuance or recess, prohibit the party from introducing evidence not disclosed, or impose other sanctions for failure to comply with discovery orders. N.C. Gen. Stat. § 15A-910(a)(2) (2011).

However, the "Sixth Amendment [of the United States Constitution] 'guarantees a defendant's right to confront those "who bear testimony" against him.' *Melendez-Diaz*, 557 U.S. at ___, 174 L. Ed. 2d at 321 (quoting *Crawford*, 541 U.S. at 51, 124 S.Ct. 1354, 158 L. Ed. 2d at 193)." *State v. Galindo*, 200 N.C. App. 410, 413, 683 S.E.2d 785, 787 (2009). The Sixth Amendment also guarantees a defendant's right to present a defense: "Just as an accused has the right to confront the prosecution's witnesses for the purpose of challenging their testimony, he has the right to present his own witnesses to establish a defense. This right is a fundamental element of due process of law." *Washington v. Texas*, 388 U.S. 14, 19, 18 L. Ed. 2d 1019, 1023 (1967).

> The United States Supreme Court addressed the issue of whether the refusal to allow an undisclosed witness to testify violated the petitioner's constitutional right to obtain the testimony of favorable witnesses in *Taylor v. Illinois*, 484 U.S. 400, 98 L.Ed.2d 798. In *Taylor*, the United States Supreme Court stated that "'criminal defendants have

> the right to the government's assistance in compelling the attendance of favorable witnesses at trial and the right to put before a jury evidence that might influence the determination of guilt.'" "Few rights are more fundamental than that of an accused to present witnesses in his own defense. Indeed, this right is an essential attribute of the adversary system itself."

State v. Gillespie, 180 N.C. App. 514, 519, 638 S.E.2d 481, 485 (2006) *review allowed*, *writ allowed*, 361 N.C. 362, 646 S.E.2d 369 (2007), *and adopted as modified*, 362 N.C. 150, 655 S.E.2d 355 (2008).

The United States Supreme Court has stated that rules of evidence

> do not abridge an accused's right to present a defense so long as they are not 'arbitrary' or 'disproportionate to the purposes they are designed to serve.' Moreover, we have found the exclusion of evidence to be unconstitutionally arbitrary or disproportionate only where it has infringed upon a weighty interest of the accused.

United States v. Scheffer, 523 U.S. 303, 308, 140 L. Ed. 2d 413, 418-19 (1998) (citations omitted). Therefore, a defendant has a constitutional right to present otherwise admissible expert witness testimony if that testimony is "'likely to be a significant factor' in the defense." *Tucker*, 329 N.C. at 718-19, 407 S.E.2d at 811 (citations omitted).

In the present case, the only evidence presented by the State directly linking Defendant to the murder was the evidence of the Google Map search pinpointing the location where Ms. Cooper's body was found. Evidence challenging the State's presentation of that evidence would have clearly been a "significant factor" in Defendant's defense. Defendant was barred from presenting any evidence from his own witnesses concerning the Google Map files recovered from the laptop.

> The right of the defendant to present evidence "stands on no lesser footing than the other Sixth Amendment rights that we have previously held applicable to the States." We cannot accept the State's argument that this constitutional right may never be offended by the imposition of a discovery sanction that entirely excludes the testimony of a material defense witness.

Taylor, 484 U.S. at 409, 98 L. Ed. 2d at 810-11 (citations omitted).

We assume, *arguendo*, that Defendant technically violated N.C.G.S. § 15A-905. Though exclusion of Masucci's testimony may not have been arbitrary, we hold that it was disproportionate to the purposes this state's discovery rules were intended to serve. Our Supreme Court found that denial of funds to an indigent defendant to obtain an expert witness was unconstitutional for the following reasons:

> In the present case, defendant demonstrated that the determination of his guilt or

> innocence would hinge largely on the unrebutted testimony of the state's fingerprint expert. Defendant requested a fingerprint expert not to engage in some amorphous fishing expedition . . . but to enable him, and ultimately perhaps the jury, to assess more accurately the one item of hard evidence implicating him in the crimes charged. Under these circumstances, denying defendant the assistance of a fingerprint expert denied him "an adequate opportunity to present his claims fairly within the adversary system."

State v. Moore, 321 N.C. 327, 347, 364 S.E.2d 648, 656 (1988) (citation omitted). All else being equal, the prejudice to a defendant is the same whether he is prevented from presenting expert testimony due to indigence, or as a sanction for discovery rules violations.

The United States Supreme Court determined in *Taylor* that:

> A trial judge may certainly insist on an explanation for a party's failure to comply with a request to identify his or her witnesses in advance of trial. If that explanation reveals that the omission was willful and motivated by a desire to obtain a tactical advantage that would minimize the effectiveness of cross-examination and the ability to adduce rebuttal evidence, it would be entirely consistent with the purposes of the Compulsory Process Clause simply to exclude the witness' testimony. *Cf. United States v. Nobles*, 422 U.S. 225, 45 L. Ed. 2d 141 (1975).

Taylor, 484 U.S. at 415, 98 L. Ed. 2d at 814 (footnote omitted). However, the Court's later holding in *Michigan v. Lucas* stated:

> We did not hold in *Taylor* that preclusion is

> permissible every time a discovery rule is violated. Rather, we acknowledged that alternative sanctions would be "adequate and appropriate in most cases." We stated explicitly, however, that there could be circumstances in which preclusion was justified because a less severe penalty "would perpetuate rather than limit the prejudice to the State and the harm to the adversary process." *Taylor*, we concluded, was such a case. The trial court found that Taylor's discovery violation amounted to "willful misconduct" and was designed to obtain "a tactical advantage." Based on these findings, we determined that, "[r]egardless of whether prejudice to the prosecution could have been avoided" by a lesser penalty, "the severest sanction [wa]s appropriate."

Michigan v. Lucas, 500 U.S. 145, 152, 114 L. Ed. 2d 205, 214 (1991) (citations omitted). The First Circuit has presented the rationale of *Taylor* in a way we find instructive:

> Although the *Taylor* Court declined to cast a mechanical standard to govern all possible cases, it established that, as a general matter, the trial judge (in deciding which sanction to impose) must weigh the defendant's right to compulsory process against the countervailing public interests: (1) the integrity of the adversary process, (2) the interest in the fair and efficient administration of justice, and (3) the potential prejudice to the truth-determining function of the trial process. The judge should also factor into the mix the nature of the explanation given for the party's failure seasonably to abide by the discovery request, the willfulness *vel non* of the violation, the relative simplicity of compliance, and whether or not some unfair tactical advantage has been sought.

Chappee v. Vose, 843 F.2d 25, 29 (1st Cir. 1988) (citations omitted).

Defendant, in failing to provide earlier notice to the State, was clearly not seeking any tactical advantage. The trial court made no finding of willful misconduct, and the record divulges none. Defendant only sought out another expert, Masucci, after the State was successful in moving to limit Ward's testimony in the middle of the trial. At that point, Defendant had no way to present vital expert testimony and comply with N.C.G.S. § 15A-905(c)(2).

In light of the lack of willful misconduct on the part of Defendant, the rational reason presented for failing to inform the State before trial that Defendant would be calling Masucci, the role of the State in having this situation arise after the trial had commenced, the fundamental nature of the rights involved, the importance to the defense of the testimony excluded, and the minimal prejudice to the State had the trial court imposed a lesser sanction – such as continuance or recess, we hold that imposing the harsh sanction of excluding Masucci from testifying constituted an abuse of discretion. Assuming, *arguendo*, there was no abuse of discretion, we hold that excluding Masucci's testimony as a sanction for a discovery

rules violation violated Defendant's rights under the constitutions of the United States and North Carolina.

Pursuant to either standard, we hold that the error was of such magnitude, in light of the earlier exclusion of Ward's relevant testimony, that it requires Defendant be granted a new trial.

IV. Denial of Motion for Discovery

In Defendant's third argument, he contends the trial court erred in denying his motions for discovery of certain evidence contained in the files of some of the State's witnesses.

"Questions concerning discovery must be resolved by reference to statutes and due process principles, as no right to pretrial discovery existed at common law." *State v. McDougald*, 38 N.C. App. 244, 254, 248 S.E.2d 72, 81 (1978) (citations omitted); see also, *State v. Cunningham*, 108 N.C. App. 185, 195-96, 423 S.E.2d 802, 808-09 (1992). "Discovery, like cross-examination, minimizes the risk that a judgment will be predicated on incomplete, misleading, or even deliberately fabricated testimony." *Taylor*, 484 U.S. at 411-12, 98 L. Ed. 2d at 812.

N.C. Gen. Stat. § 15A-903 controls discovery required to be provided by the State. N.C.G.S. § 15A-903 has been amended

twice since Defendant was indicted in this matter. The version of N.C.G.S. § 15A-903 relevant to this appeal stated:

> (a) Upon motion of the defendant, the court must order the State to:
>
> (1) Make available to the defendant the complete files of all law enforcement and prosecutorial agencies involved in the investigation of the crimes committed or the prosecution of the defendant. The term "file" includes the defendant's statements, the codefendants' statements, witness statements, investigating officers' notes, results of tests and examinations, or any other matter or evidence obtained during the investigation of the offenses alleged to have been committed by the defendant. The term "prosecutorial agency" includes any public or private entity that obtains information on behalf of a law enforcement agency or prosecutor in connection with the investigation of the crimes committed or the prosecution of the defendant. . . . . The defendant shall have the right to inspect and copy or photograph any materials contained therein and, under appropriate safeguards, to inspect, examine, and test any physical evidence or sample contained therein.

N.C. Gen. Stat. § 15A-903 (2009).

Certain materials are specifically excluded from the disclosure requirement of N.C.G.S. § 15A-903:

> (a) The State is not required to disclose written materials drafted by the prosecuting attorney or the prosecuting attorney's legal staff for their own use at trial, including witness examinations, voir dire questions, opening statements, and closing arguments. Disclosure is also not required of legal research or of records, correspondence,

> reports, memoranda, or trial preparation interview notes prepared by the prosecuting attorney or by members of the prosecuting attorney's legal staff to the extent they contain the opinions, theories, strategies, or conclusions of the prosecuting attorney or the prosecuting attorney's legal staff.

N.C. Gen. Stat. § 15A-904 (2009). However,

> N.C. Gen. Stat. § 15A-903 provides that criminal defendants have broad pretrial access to discovery of materials obtained or prepared for the prosecution for use in its case in chief, including "not only conclusory laboratory reports, but also any tests performed or procedures utilized by chemists to reach such conclusions." This is due to "the extraordinarily high probative value generally assigned by jurors to expert testimony . . ."

State v. Llamas-Hernandez, 189 N.C. App. 640, 652–53, 659 S.E.2d 79, 86–87 (2008) (Steelman, J., dissenting), *reversed per curiam for the reasons stated in the dissent*, 363 N.C. 8, 673 S.E.2d 658 (2009) (citations omitted). As stated by the United States Supreme Court:

> Cross-examination is the principal means by which the believability of a witness and the truth of his testimony are tested. Subject always to the broad discretion of a trial judge to preclude repetitive and unduly harassing interrogation, the cross-examiner is not only permitted to delve into the witness' story to test the witness' perceptions and memory, but the cross-examiner has traditionally been allowed to impeach, *i.e.*, discredit, the witness.

Davis v. Alaska, 415 U.S. 308, 316, 39 L. Ed. 2d 347, 353 (1974) (citations omitted).

Defendant in this case moved the trial court to compel discovery of, "FBI CART (Computer Analysis Response Team) policies and procedures for the viewing, extraction or examination of digital data;" "[m]echanism of examination or extraction to include hardware and software used;" "underlying and resultant data along with examiners' or technicians' bench notes – whether handwritten, dictated or printed as well as accompanying sketches, printed screenshots, data whether printed or handwritten, photographs or video;" "complete details as to the examiner's examination of each of the files that were modified after they were taken into exclusive law enforcement custody to determine what was modified;" and other potential information or opinion concerning the laptop in the records of CART personnel. The State filed a motion in opposition, arguing that there exists "a law enforcement sensitive qualified evidentiary privilege" which should act to prevent discovery of these items, "because such disclosure could lead to the development of countermeasures to FBI investigative techniques. Such countermeasures could defeat law enforcement's ability to obtain forensic data in criminal cases." The State also argues that this information was protected as "work product."

The trial court denied Defendant's motion to compel discovery by order entered 4 October 2010. The trial court found as fact "[t]hat the FBI's Standard Operating Procedures and policies are the same techniques and tools that are used in counterterrorism and counterintelligence investigations[.]" The trial court concluded that "under the provisions of N.C. Gen. Stat. § 15A-903, patterned after Federal Rule of Criminal Procedure 16, the disclosure of the information sought by . . . Defendant would be contrary to the public interest in the effective functioning of law enforcement[,]" and that "under the provisions of N.C. Gen. Stat. § 15A-908[,]" disclosure of the information would result in "substantial risk" of harm to "any person, including the citizens of this State, of physical harm." The trial court did not deny Defendant's motion based upon "work product" privilege.

N.C. Gen. Stat. § 15A-908(a) states in relevant part:

> Upon written motion of a party and a finding of good cause, which may include, but is not limited to a finding that there is a substantial risk to any person of physical harm, . . . the court may at any time order that discovery or inspection be denied, restricted, or deferred, or may make other appropriate orders.

N.C. Gen. Stat. § 15A-908 (2011). We have no way to evaluate the trial court's order denying discovery of the requested FBI's standard operating procedures and policies as there is nothing

in the record indicating what these procedures and policies are or how making them discoverable would compromise the FBI's ability to conduct future investigations. The trial court could have conducted an *in camera* review of the requested discovery, and sealed the portions withheld to include in the record on appeal for this Court to review. *See State v. Vandiver*, 321 N.C. 570, 571-72, 364 S.E.2d 373, 374 (1988). Even in the face of a compelling State interest in keeping records confidential, due process might compel discovery, depending on how material the records are to a defendant's defense. *Pennsylvania v. Ritchie*, 480 U.S. 39, 56-58, 94 L. Ed. 2d 40, 56-58 (1987); *United States v. Nixon*, 418 U.S. 683, 712, 41 L. Ed. 2d 1039, 1066 (1974) ("the allowance of the privilege to withhold evidence that is demonstrably relevant in a criminal trial would cut deeply into the guarantee of due process of law and gravely impair the basic function of the courts"). We hold that on these facts due process required that the trial court at least examine the records *in camera* to determine whether they should be provided to the defense. *See Ritchie*, 480 U.S. at 56-58, 94 L. Ed. 2d at 56-58.

We do not question that N.C.G.S. § 15A-908 may serve to prevent discovery of certain otherwise discoverable materials, based upon the *concerns* argued in the present case. In this

case, however, we find the blanket exclusion ordered by the trial court unsupported by the record we have before us. When cross-examination of a key State's witness is going to potentially be limited by exclusion of certain discovery in a first-degree murder trial, a more particularized and focused order is warranted. Furthermore, this determination cannot be made if the trial court does not evaluate the contested evidence. Finally, sufficient record of the excluded materials should be preserved for appellate review. *See State v. Brown*, 116 N.C. App. 445, 446-47, 448 S.E.2d 131, 132-33 (1994).

As one example of the over-broad nature of the trial court's order, and the implementation of that order, Special Agent Johnson testified that the CART team conducted a test to try to replicate the data produced by the purported Google Map search conducted on Defendant's laptop. When the defense attempted to obtain information regarding that test, the following exchange occurred:

> [MR. KURTZ – Defendant's attorney]. And when you let go of the cursor at the end of the navigation, is that consistent with when the last accessed time occurs?
>
> [Special Agent Johnson]. Again, it's -- it's my recollection on those tests that -- to answer your question, no. It was the time that we clicked on the -- the left button to close the hand. That was when the file was downloaded and those were the -- those were the consistent dates across the

board. So if -- if we - - if we had went back and used that icon again, that closed hand function, it did not update those dates -- or the times. They were all reflected of when they were first initiated.

Q. Do you still have that test data?

A. I'm sure we do. I -- I believe that was a large part of Officer Chappell's testimony.

Q. Is there any -- is -- the test data that resulted from Officer Chappell and your testing, is that particular data in any way a jeopardy to national security if it was disclosed to us?

MR. ZELLINGER: Your Honor, I'm going to object. This is far outside the scope of determining whether that computer is proper for an examination. And -- and we're also delving into a -- an issue of law here for the Court and not for Agent Johnson.

MR. KURTZ: Well, Judge, there is potentially a piece of information that exists on Mr. Cooper's computer that could say definitely that this material was planted, absolutely definitive. I may be wrong. Special Agent Johnson's testing may indeed be that it all has the exact same millisecond all the way across. I don't think I'm wrong. Now, one way or the other, whether it's having a -- a test done on a Vista machine now and seeing what it -- what it actually shows or giving us access to the original test data, which I don't believe has any national security ramifications since it deals with a Google Map test. One way or the other, we should be entitled to this information as it could be tremendously exculpatory.

THE COURT: Upon reconsidering this issue about this in-court test, pursuant to Rule

403, I'm going to sustain the objection and exclude any testing in Court because of the differences in the equipment and the statements made by this witness that this is not the appropriate place to do it. We need to bring the jury back in. And regarding the national security issue, that is a matter that we have already ruled on. It is something I have already dealt with.

MR. KURTZ: But, Your Honor, there is a witness on the stand that can answer specifically whether this is an issue of national security. And I'm not even going to be allowed to ask that question?

THE COURT: I believe I've already determined, because of the rules of the -- and the discovery process that you are not entitled to get those things.

MR. KURTZ: So my understanding is, the -- the rules and the discovery process, we're hiding behind national security on an issue where we could get a clear answer from a witness that this is not in fact a national security issue. And we're talking about a piece of information that could be exculpatory to Mr. Cooper.

MR. ZELLINGER: Your Honor, first of all, the exculpatory information is already in the Defendant's possession. He has all the files. The fact that his expert is -- his alleged expert can't speak to that is what the issue is before the Court. But as to any exculpatory information, all that has been given to the Defendant. All those computer files have been given to the Defendant. So I -- I want to just take issue with that and I -- I just wanted to put that on the record, as to the rest regarding –

MR. KURTZ: Your Honor, that -- that is an inaccurate statement because we're not

talking about data from this computer. We're –

. . . .

MR. KURTZ: We're talking about data that Special Agent Johnson and Officer Chappell generated when they attempted to replicate the search. When they did -- when -- replicated this search, they will have generated -- and in fact, we've got a screen shot that shows the first of the timestamps. There are additional timestamps that are off screen. Those additional timestamps would answer this question definitely. And there can be no national security issue here, given we're talking about Mr. Cooper's computer alone and the data that was generated during their testing.

THE COURT: It's the methodology that they used, I think, that falls under the security issue, but –

MR. KURTZ: But if I could ask Special Agent Johnson if he has any national security concerns related to that methodology, we might be able to determine that this one particular test is a legitimate one to be disclosed, that it will not actually disclose the missile codes.

MR. ZELLINGER: Your Honor, I'm looking at the -- the affidavit of the FBI agent who provided an affidavit to the Court on June 10th of 2010. And -- and that set out the FBI current policies and procedures for the viewing, extraction, and or examination of digital data, the FBI's policies on the analysis, or -- or how it was -- how it was examined, numerous other documents from FBI Special Agent Johnson pertaining to his examination of the computers in this case, including but not limited to, communications logs, examiner bench notes, and all other

> documents completed or compiled by Special Agent Johnson beyond the report of the examination. That's what we're seeking to protect here, because we don't want, pursuant to state case law, we -- the standard operating procedures of the FBI are protected throughout our nation. And we're not hiding behind anything. All that information's been given to the Defendant. Agent Johnson's given out more information in this case than he's ever given out in any other case. And as to the -- the specific material that the Defendant wants, he has these files. If -- if their [sic] exculpatory, take them to an expert and find out how [they're] exculpatory. But the fact is that these files the Defendant has in his possession. Asking Agent Johnson on voir dire about national security just seems wildly inappropriate to me, and then he wants to know exactly how every part of every test that Agent Johnson does can affect national security and that people could be put in danger or child pornography could - could easily be deleted after this information comes out. And we're re-litigating this issue again.
>
> MR. KURTZ: Your Honor, what Mr. Zellinger is saying is -- is flat out dishonest and is ascertainable by asking Special Agent Johnson if this is information that we ever got. He's saying we have these files; we don't have these files. These are not the files from Mr. Cooper's computer. These are the files from Special Agent Johnson and Chappell's tests.
>
> THE COURT: The objection is sustained. I'm not going to allow further questioning in this line or any in-court testing of that computer. We need to bring in the jury.

It was error for the trial court to shut down this line of questioning without ascertaining how, or if, national security

or some other legitimate interest outweighed the probative value of this information to Defendant. On remand, the trial court must determine with a reasonable degree of specificity how national security or some other legitimate interest would be compromised by discovery of particular data or materials, and memorialize its ruling in some form allowing for informed appellate review.

New trial.

Judges GEER and DAVIS concur.