STATE OF INDIANA) IN THE HAMILTON COUNTY SUPERIOR COURT NO. 3
) SS:
COUNTY OF HAMILTON) CAUSE NO. 29D03-2109-PL-__________

CINDY GOSSARD, CLERK-TREASURER,)
CITY OF WESTFIELD, INDIANA,)
)
Plaintiff,)
)
v.)
)
J. ANDREW COOK, MAYOR, CITY OF)
WESTFIELD, INDIANA,)
)
Defendant.)

CLERK-TREASURER GOSSARD'S COMPLAINT FOR DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

COMES NOW, the Plaintiff, Cindy Gossard, Clerk-Treasurer of the City of Westfield, Indiana ("Clerk-Treasurer Gossard"), by counsel, and for her Complaint for Declaratory Judgment against the Defendant, J. Andrew Cook, Mayor of the City of Westfield, Indiana ("Mayor Cook"), alleges and states as follows:

PARTIES, JURISDICTION & VENUE

1. Cindy Gossard is the Clerk-Treasurer of the City of Westfield, State of Indiana, a third-class city located in Hamilton County, Indiana.

2. J. Andrew Cook is the Mayor of the City of Westfield, State of Indiana, a third-class city located in Hamilton County, Indiana.

3. Clerk-Treasurer Gossard is the duly elected, independent Clerk-Treasurer of the City of Westfield, and acts as both the clerk and the fiscal officer of the City of Westfield.

4. Indiana Code § 36-4-10-4 and Indiana Code § 36-4-10-4.5 outline the core enumerated powers held by Clerks and Fiscal Officers.

5. Specifically, Clerk-Treasurer Gossard is statutorily required to:

a. maintain all records required by law (Ind. Code § 36-4-10-4(2)); receive and care for all city money (Ind. Code § 36-4-10-4.5(1));

b. keep accounts showing when and from what sources the fiscal officer has received city money and when and to whom the fiscal officer has paid out city money (Ind. Code § 36-4-10-4.5(2));

c. prescribe payroll and account forms for all city offices(Ind. Code § 36-4-10-4.5(3));

d. prescribe the manner in which creditors, officers, and employees shall be paid (Ind. Code § 36-4-10-4.5(4));

e. manage the finances and accounts of the city and make investments of city money (Ind. Code § 36-4-10-4.5(5)); and

f. perform all other duties as prescribed by statute (Ind. Code § 36-4-10-4(5), Ind. Code § 36-4-10-4.5(9)).

6. As the City's Executive, Mayor Cook and/or his Office is the supervisor of the City's IT Department.

7. As alleged herein, Mayor Cook has taken actions to invade and encroach upon the statutory powers of Clerk-Treasurer Gossard by installing software onto the computers of the Clerk-Treasurer's Office that allow Mayor Cook, his administration, and third-parties access into the financial and data systems that are required to be maintained by Clerk-Treasurer Gossard, without any authorization or permission from Clerk-Treasurer Gossard.

8. Because this case involves a dispute regarding the nature and extent of the statutory powers and duties of the executive branch and Clerk-Treasurer Gossard's Office, this Court has jurisdiction under Indiana Code § 36-4-4-5.

9. Hamilton County is the preferred venue under Trial Rule 75(A)(5) and pursuant to Indiana Code § 36-4-4-5.

FACTUAL BACKGROUND

10. Clerk-Treasurer Gossard maintains all records of the City and administers and maintains the City's financial systems, including the ADP payroll system and the City's Microsoft Navigator account, which contains the records of all City financial transactions, and oversees and manages all City financial accounts, such as bank accounts for purchase-credit cards ("P-Cards") used by City employees.

11. While various departments and employees of the City may also use these systems and databases for various reasons, Clerk-Treasurer Gossard and her Office retain sole administrator-level access to such databases systems.

12. Administrator-level access differs from "view-only" access, in that view-only access gives a user permission to see information and in certain circumstances make data entries, whereas administrator-level access allows a user to not only enter data, but also provides the ability to edit, manipulate, or delete data.

13. Mayor Cook has sought to usurp and undermine Clerk-Treasurer Gossard's statutory duty to maintain the integrity and security of City records and financial databases through various avenues of attack since September of 2020.

Attempts to Gain Administrator-Level Access through Statutory Examination.

14. On or about August 7, 2020, Mayor Cook ordered an examination for the purported purpose of examining City accounts.

15. Beginning on or about September 2, 2020, Mayor Cook has demanded administrator-level access into the financial systems and databases maintained by Clerk-Treasurer Gossard.

16. On or about September 2, 2020, Mayor Cook's examiners demanded administrator credentials for the City's ADP Account, the City's Microsoft Navigator Account, and the City's Account with Chase MasterCard.

17. In response, Clerk-Treasurer Gossard agreed to provide requested information but declined to provide administrator credentials that would allow for administrator-level access into such systems, in accordance with executing her statutory duties.

18. On or about October 14, 2020, Mayor Cook's examiners again demanded credentials for the City's ADP Account, the City's Microsoft Navigator Account, and the City's Account with Chase MasterCard.

19. Clerk-Treasurer Gossard again declined to provide administrator credentials that would allow for administrator-level access into such systems, but agreed to continuing to work cooperatively to provide requested information in a "view-only" form.

20. On or about October 23, 2020, Clerk-Treasurer Gossard continued to cooperate with the examination by providing the information being requested by Mayor Cook's examination by providing the examiners with a flash drive containing additional information and data that was being requested.

21. After providing much of the information requested, but continuing to execute her statutory duty of maintaining the integrity of City financial systems and databases by continuing to decline to provide administrator-level access to City financial systems, one of Mayor Cook's appointed examiners, Taft Attorney Zachary Klutz, requested the service contract for the ADP payroll service from the Clerk-Treasurer's Office on or about October 30, 2020.

22. On or about November 5, 2020, the Clerk-Treasurer's Office provided Attorney Klutz with the requested ADP master services contract.

23. The master services contract between ADP and the City was originally executed in August 2008, and had been in place continuously without any issues as to the legality of the contract since it was originally executed.

24. On or about November 19, 2020, Mayor Cook's Chief of Staff, Todd Burtron, issued correspondence to ADP's general counsel, in which Mayor Cook alleged, for the first time in the history of the contract's existence, that 2008 ADP master services agreement was legally void; this same correspondence invited ADP to execute a new contract with the City, which would name Mayor Cook as the administrator of the account; and Mayor Cook advised ADP that the Clerk-Treasurer would "be granted access" *after* Mayor Cook received administrator log-in credentials.

25. ADP thereafter refused to modify the original 2008 master services agreement without the consent of Clerk-Treasurer Gossard.

26. Clerk-Treasurer Gossard continued to cooperate with the requests from Mayor Cook's examiners by providing information and data requested, but did so by providing such information in a "view-only" format only, and consistently refused to provide administrator-level access.

Attempts to Gain Administrator-Level Access through Legal Action.

27. On January 14, 2021, Mayor Cook filed a Complaint for Declaratory Judgment and Injunctive Relief[1] pursuant to Indiana Code § 36-4-4-5, in which Mayor Cook sought an injunction ordering Clerk-Treasurer Gossard to "cooperate with the Investigation and to provide *all information and <u>access</u>*" being requested by Mayor Cook and his examiners.

28. In conjunction with his lawsuit, Mayor Cook sought a temporary restraining order against Clerk-Treasurer Gossard, in which Mayor Cook made the primary purpose of his lawsuit clear by including the following language in a proposed order for granting of temporary restraining order:

> "[T]he Clerk-Treasurer shall provide Mayor Cook and his staff *<u>unlimited access</u> to <u>all</u> payroll and financial information* of the City contained within ADP *or otherwise*, and that the Clerk-Treasurer shall *immediately and <u>fully cooperate</u>* with the Appointees and the Investigation." (Emphasis supplied.)

29. Given her statutory duties, Clerk-Treasurer Gossard vigorously defended Mayor Cook's lawsuit, especially with respect to Mayor Cook's attempt to seek full and unfettered administrator-level access into the City's financial systems that Clerk-Treasurer Gossard is required to securely maintain.

30. Just as she had prior to the instigation of Mayor Cook's lawsuit, Clerk-Treasurer Gossard continued to cooperate with Mayor Cook's examination by providing the examiners with any information and data requested in a "view-only" format, while continuing to refuse to provide administrator-level access to financial systems and information; examples of such cooperative efforts include, but are not limited to:

[1] *See*, Cause Number 29D02-2101-PL-000268.

a. on or about January 26, 2021, Clerk-Treasurer Gossard's Office provided ADP data files in a "view-only" format to Mayor Cook's examiners;

b. on or about January 26, 2021, Clerk-Treasurer Gossard's Office refused to provide login credentials to the City's online banking accounts for security purposes, but committed to making the information itself available at an on-site inspection;

c. on or about January 26, 2021, Clerk-Treasurer Gossard's Office sent copies of bank statements and cancelled checks to the examiners;

d. on or about February 12, 2021, Clerk-Treasurer Gossard provided access to the Clerk-Treasurer's Office so that the examiners could perform an on-site data extraction of various forms of financial data under supervision of Clerk-Treasurer Gossard's staff and legal counsel;

e. on or about February 18, 2021, Clerk-Treasurer Gossard provided access to the Clerk-Treasurer's Office to the examiners for a second on-site data extraction where additional data was provided;

f. on or about February 26, 2021, Clerk-Treasurer Gossard's legal counsel provided bank account statements to the examiners pursuant to a request for the same; and

g. on or about March 9, 2021, Clerk-Treasurer Gossard's legal counsel provided ADP reports based on custom report parameters as requested by the examiners.

Mayor Cook's Sudden Change of Position Regarding Administrator-Level Access.

31. On or about March 16, 2021, the parties appeared before Hamilton Superior Court No. 2 for hearing on Gossard's Motion to Certify Order for Interlocutory Appeal; following argument and the Court entering an order of denial as to Gossard's Motion, an impromptu status conference was conducted on the record, during which counsel for Mayor Cook advised, *for the first time since September 2020*, that Mayor Cook would be satisfied with access to the City's ADP and Microsoft Navigator accounts, and other financial data, on a "view-only" permission basis.

32. On or about March 23, 2021, counsel for Clerk-Treasurer Gossard corresponded to Mayor Cook's counsel to advise that the Clerk-Treasurer did not oppose providing access to the City's ADP and Microsoft Navigator Accounts on a "view-only" permission basis, and further requested information necessary for establishing such access.

33. The parties thereafter worked cooperatively to establish "view-only" access for Mayor Cook and City administrators to the various financial systems and databases maintained by the Clerk-Treasurer's Office, which efforts included setting up specific limited-permission accounts to such systems and coordinating training sessions for administration officials and employees within the ADP and Microsoft Navigator systems.

34. The aforementioned efforts on the part of Clerk-Treasurer Gossard resulted in Mayor Cook and his Administration having access to the City's financial systems and databases, including ADP and Microsoft Navigator Accounts, on a strictly "view-only" basis.

35. As a result, the then-existing claims and controversies of the pending litigation had been resolved, and the parties therefore entered and filed a Joint Stipulation of Dismissal on

or about May 24, 2021, which resulted in dismissal of the action by Hamilton County Superior Court No. 2 on May 25, 2021.

Unbeknownst to Clerk-Treasurer Gossard, Mayor Cook No Longer Required Administrator-level Access Credentials Because Mayor Cook Had Established Covert Back-Door Access into the City's Financial Systems Using "Unattended Remote Access Software."

36. During the pendency of Mayor Cook's lawsuit in early 2021, staff members in the Clerk-Treasurer's Office began to notice occasional oddities and/or "glitches" occurring with their computers – examples of such events include mouse icons moving across staff member computer screens without mouse input from the staff member, programs being opened without prompting, and staff members being unable to locate electronic files or data that they had individually created.

37. Then, on or about April 15, 2021, a staff member in the Clerk-Treasurer's Office discovered that the web browser on her local computer had saved, or "remembered," a login user ID, which was displayed as an email address for one a member of Mayor Cook's examination team; this particular discovery was highly suspicious in that the member of the examination team had not been given direct access to the computer in question by anyone in the Clerk-Treasurer Gossard's Office.

38. On or about April 28, 2021, the Clerk-Treasurer examined six computers in the Clerk-Treasurer's Office, and discovered a software program running called "Remote Support Jump Client 20.1.1," which program had an installation date of November 18, 2020; in addition, two newer laptop computers that had been provided to the Clerk-Treasurer's staff on April 14, 2021, and April 25, 2021, were found to have this same software program preinstalled.

39. Upon information and belief, the software program in question is from a company called Beyond Trust, which markets this software program for "unattended remote access"; this

software differs from traditional remote access technology in that it does not require a local user to grant permission to an outside user to initiate a remote access session.

40. Upon information and belief, Beyond Trust markets its "Jump" software as having the following relevant capabilities:

a. "Jump" is the term for all Beyond Trust unattended access technologies – "unattended access" refers to accessing remote systems without requiring interaction from a remote user to initiate access;

b. "File Transfer" allows for the transferring of files to and from a remote computer;

c. "Remote Screenshot" allows the user to capture screenshots of the display of a target remote computer;

d. "View or Control" features allow the user to either view or take control of a remote computer;

e. "Wake-on-Lan" feature allows a user to remotely access a target computer even when the target computer is turned off and powered down;

f. "Vault Discovery" feature allows a user to discover login credentials within a targeted computer, which can then be imported into Vault, enabling users to inject and use the discovered credentials within a remote support session;

g. "Beyond Trust Vault" uses the built-in Beyond Trust credential manager to store and inject credentials into support sessions;

h. "Jump Client Discovery & Rotation" feature allows a user to perform discovery and rotation of local credentials on a target computer, which allows to create access into a local computer without the need to set up a local or shared account on the local computer itself; and

i. "Favorite Credentials Used for Injection" feature gives the user's console the ability to display the most likely user credentials needed for credential injection based on usage history and account permissions.

41. Following discovery of the software, counsel for Clerk-Treasurer Gossard made a request to the City Attorney, Blake Burgan, to have the software removed, which request was denied.

42. On or about May 21, 2021, Clerk-Treasurer Gossard issued correspondence to Mayor Cook advising of the discovery of the Beyond Trust software, advising that due to this software, Clerk-Treasurer Gossard could not ensure the security of who was accessing the City's financial systems, and requesting that the City IT department immediately remove the Beyond Trust software and all related software.

43. On or about June 4, 2021, City Attorney Blake Burgan issued responsive correspondence to counsel for Clerk-Treasurer Gossard, in which he advised that Mayor Cook and the City Administration vehemently denied "all allegations."

The Clerk-Treasurer Initiates Investigation and the Administration's Illegal Raid of the Clerk-Treasurer's Office.

44. Following the Administration's "vehement denial," Mayor Cook and Administration officials have continued to deny any wrongdoing, have denied the use of "spyware" against the Clerk-Treasurer's Office, and has generally maintained that the Beyond Trust software found on the computers in the Clerk-Treasurer's Office constitutes "normal and routine IT support" efforts.

45. Based on these denials, and in furtherance of her statutory duties, Clerk-Treasurer Gossard resolved to examine the use of the software on the computers in the Clerk-Treasurer's Office.

46. Accordingly, on or about July 1, 2021, counsel for the Clerk-Treasurer advised City Attorney Blake Burgan of the Clerk-Treasurer's intention to conduct said examination, and further advised the City Attorney that Clerk-Treasurer Gossard was interviewing forensic information technology firms for that purpose.

47. On or about July 6, 2021, counsel for the Clerk-Treasurer advised City Attorney Blake Burgan that the Clerk-Treasurer had been speaking with different IT companies and "has someone that is looking into the issue."

48. On or about July 23, 2021, Clerk-Treasurer Gossard retained Veracity IIR to conduct an examination into the use of the Beyond Trust software with respect to the computers in the Clerk-Treasurer's Office; the scope of Veracity IIR's work was limited to examining the hard drives of the computers only, and did not involve examination or entry into the City's computer networks or systems generally.

49. On or about July 23, 2021, Clerk-Treasurer Gossard authorized Veracity IIR to enter the Clerk-Treasurer's Office for the purpose of forensically imaging the hard drives of the computers used by Clerk-Treasurer Gossard and her staff.

50. On or about July 23, 2021, Veracity IIR began the process of forensically imaging the hard drives of said computers by disconnecting the hard drives from the computer machines, and running an imaging program to replicate exact copies of the current states of the hard drives in question; at all times during said imaging, the hard drives of each computer were fully and

completely disconnected from the City's computer network, and were otherwise disconnected from any internet and/or intranet source during the imaging.

51. On or about July 26, 2021, Clerk-Treasurer Gossard authorized Veracity IIR to return to the Clerk-Treasurer's Office to continue the forensic imaging process by completing said imaging on the remaining hard drives whose imaging were not completed on July 23, 2021.

52. On that same evening of July 26, 2021, the Westfield City Council held a regularly scheduled public meeting.

53. The Westfield City Council conducts its public meetings in the Council's assembly room, which is located directly above the Clerk-Treasurer's Offices.

54. During the course of the July 26, 2021, Council public meeting, Clerk-Treasurer Gossard addressed the Council and the public, and advised that the Clerk-Treasurer's efforts to investigate the use of the Beyond Trust software within the Clerk-Treasurer's Office was underway, and further advised that she would publicly update the Council upon completion of the examination.

55. Immediately following Clerk-Treasurer Gossard's public comments during the July 26, 2021, Council meeting, Director of the City's IT Department, Christopher Larsen ("Larsen"), answered questions from the Council regarding the use of the Beyond Trust software; Larsen advised the Council that the program in question was standard IT support software, and that any use of such software would be clearly identifiable and known to any end user; however, Larsen went on to admit to the Council that his department does, in fact, have the ability to access local computers without the local user's knowledge and permission.

56. On July 26, 2021, after the conclusion of the City Council's public meeting, and after participants and attendees had left the premises, Larsen (and potentially other unknown

individuals) made entry into the locked Clerk-Treasurer's Office, without the Clerk-Treasurer's permission.

57. Upon information and belief, Larsen, under the apparent authority and color of state law, then proceeded to execute an unlawful search of the Clerk-Treasurer's Office.

58. Upon information and belief, Larsen – who had just been advised by Clerk-Treasurer Gossard during the public meeting that evening that her examiner's work was underway – "discovered" the forensic imaging equipment belonging to Veracity IIR, and proceeded to execute an unlawful seizure of Veracity IIR's equipment and the hard drives belonging to the computers in the Clerk-Treasurer's Office.

59. Upon information and belief, Larsen then proceeded to exert unauthorized control over said equipment belonging to Veracity IIR and the Clerk-Treasurer's Office, and removed it from the Clerk-Treasurer's Office.

60. On or about July 26, 2021, after conducting the unlawful search and seizure (and/or theft) described above, Larsen sent an email to Clerk-Treasurer Gossard admitting that he had made unauthorized entry into the Clerk-Treasurer's Office, admitting that he had "discovered" equipment that he had identified as not belonging to the City, and admitted to removing said equipment from the Clerk-Treasurer's Office.

61. On July 27, 2021, a criminal investigation was requested by Clerk-Treasurer Gossard; as an immediate result, on July 27, 2021, the equipment belonging to Veracity IIR was returned to Veracity IIR's possession.

62. Examination of its imaging equipment by Veracity IIR confirmed that it had completed the forensic imaging of the computer hard drives in question, and that it had secured digital copies of the hard drives of the eight computers used by the Clerk-Treasurer's Office.

The Preliminary Results of Veracity IIR's Examination into the Use of Beyond Trust Software Against the Clerk-Treasurer's Office.

63. On September 3, 2021, Veracity IIR submitted a Preliminary Report detailing preliminary findings of its forensic examination into the use of Beyond Trust software against the Clerk-Treasurer's Office. *Veracity IIR's Preliminary Report ("Report") is attached hereto as "Exhibit 1."*

64. According to Veracity IIR's Report, "[t]he Jump Client feature was installed on all computers therefore allowing remote access to each computer without requiring the local user to be present. Since this software runs in the background the local user would not be aware their actions and data files were being accessed and/or observed by a remote user. The Beyond Trust software platform also can be used to control any network cameras and microphones including the built in microphones on cameras and laptops without the local users knowledge." *See*, Exhibit 1, p. 7.

65. Veracity IIR further determine that, in addition to Beyond Trust software, a software program known as "Papercut" was discovered on the hard drives; Papercut "allows the remote admin to access digital copies of scanned and printed documents. *See*, Exhibit 1, p. 7.

66. According to Veracity IIR, "[i]f the [Clerk-Treasurer's] staff was unaware of this program it is possible sensitive information could have been observed by whomever was operating the remote user accounts with access to the papercut web portal." *See*, Exhibit 1, p. 7.

67. Veracity IIR's Report highlights additional preliminary findings, including:

a. different administrator accounts were found on the hard drives, including an account named "Informatics"[2] and "bgadmin";

[2] Upon information and belief, "Informatics" is the self-designated name of the City's IT Department headed by Christopher Larsen and under the direction and control of Mayor Cook.

b. remote support sessions using traditional means that require specific end-user permission were typically used by the Informatics admin account, whereas use of the Beyond Trust and Paperclip software programs was typically associated with the bgadmin user account;

c. 3609 data files were accessed, altered, or created by the bgadmin account during remote access sessions to computers of the Clerk-Treasurer's Office, with the majority of these files being accessed between December, 2020, and April, 2021;

d. At least 35 separate remote sessions were found to have been conducted by the bgadmin user utilizing the Beyond Trust software;

e. 220 occurrences of user bgadmin network artifacts were discovered on the computers of the Clerk-Treasurer's Office, which represent actions taken on the local computers by the remote user bgadmin;

f. 198 file records were found on the computers of the Clerk-Treasurer's Office that were associated with the Beyond Trust software and user bgadmin;

g. 1517 timeline events were extracted that were associated with the user bgadmin, and these events included remote access to files on the computers of the Clerk-Treasurer's Office, application uses, files being created/modified, review of browser history, Papercut software usage, and others; and

h. evidence that requires additional analysis also presents evidence of possible password breaking software being used remotely against the local user accounts.

68. The preliminary findings of Veracity IIR therefore present compelling evidence that Mayor Cook and his Administration have been using a software program against the Clerk-Treasurer's Office for the purpose of gaining access to the computers in the Clerk-Treasurer's Office.

69. Upon information and belief, the Beyond Trust software allows Mayor Cook and his Administration (or whomever has access to the login credentials of bgadmin) the ability to monitor and watch the computer activity of Clerk-Treasurer Gossard and her staff.

70. Upon information and belief, the Beyond Trust software allows Mayor Cook and his Administration the capability of using this remote access as a way to gain administrator-level access into the financial systems and databases that Clerk-Treasurer Gossard has a statutory duty to maintain.

71. In fact, the Beyond Trust software goes well beyond conveying administrator-level access to these systems, in that it conveys the ability to break passwords into these sensitive systems and allow its users to access the systems *under the login credentials of the Clerk-Treasurer or her staff members while remotely accessing the Clerk-Treasurer's computers*, thereby making any such access appear to be on the part of the Clerk-Treasurer's Office.

72. The existence of the Beyond Trust software on the computers of the Clerk-Treasurer's Office, and any software programs of which the Clerk-Treasurer has not been made specifically aware and consented to their use, directly interferes with the Clerk-Treasurer's

statutory duty to insure the safety and integrity of the City's financial systems and important financial data.

73. Even in the unlikely event that Mayor Cook does not have a nefarious motive for the installation and use of such software programs against the Clerk-Treasurer, the very fact that Mayor Cook has granted himself the ability to virtually access the computers in the Clerk-Treasurer's Office constitutes a brazen encroachment into the sovereignty of a separately elected government official over whom his Administration has no legal authority.

74. Therefore, *at a minimum*, the actions of Mayor Cook have interfered and continue to interfere with Clerk-Treasurer Gossard's ability to discharge her statutory duty to maintain and protect the integrity of the City's financial systems and databases.

COUNT I FOR INJUNCTIVE RELIEF

COMES NOW, Cindy Gossard, Clerk-Treasurer of the City of Westfield, Indiana, by counsel, and for Count I of her Complaint, states and alleges as follows:

75. Clerk-Treasurer Gossard incorporates, by reference, all preceding paragraphs of the present Complaint as if fully herein restated.

76. Clerk-Treasurer Gossard seeks an injunction that:

a. orders Mayor Cook and his Administration to immediately return any equipment from the Clerk-Treasurer's Office that remains in the possession of Mayor Cook and/or his Administration from the July 26, 2021, raid;

b. orders Mayor Cook and his Administration to immediately remove any and all remote access software from the computers of the Clerk-Treasurer's Office;

c. orders Mayor Cook and his Administration to remove any equipment from the Clerk-Treasurer's Office that is capable of audio recording;

d. enjoins Mayor Cook and his Administration from installing any software on the computers of the Clerk-Treasurer's Office without the express written permission of the Clerk-Treasurer;

e. enjoins Mayor Cook and his Administration from physically or electronically entering the Clerk-Treasurer's Office without the express permission of the Clerk-Treasurer; and

77. Clerk-Treasurer Gossard has no adequate remedy at law because Mayor Cook's unlawful conduct is ongoing, will continue to have significant negative impacts on Clerk-Treasurer Gossard's ability to discharge the powers and duties of her office, and will cause damage to the City and its residents that money damages will not repair.

78. Moreover, if money damages could conceivably resolve some of the issues, the process to appropriate funds and satisfy any such financial judgment would be impractical and unwieldy.

79. The balance of harms favors issuance of injunctive relief, as Clerk-Treasurer Gossard is statutorily required to maintain and safeguard the integrity of the City's financial data and information, whereas Mayor Cook does not have such statutory duties and certainly has no right to interfere with or usurp Clerk-Treasurer Gossard in the discharge of her duties.

80. The public interest in this matter will not be disserved by entry of injunctive relief; on the contrary, it is in the public's interest to insure that the Clerk-Treasurer can perform her statutory duties without interference and unlawful conduct on the part of Mayor Cook.

WHEREFORE, Cindy Gossard, Clerk-Treasurer of the City of Westfield, Indiana, respectfully requests that this Court issue an injunction that orders:

a. orders Mayor Cook and his Administration to immediately return any equipment from the Clerk-Treasurer's Office that remains in the possession of Mayor Cook and/or his Administration from the July 26, 2021, raid;

b. orders Mayor Cook and his Administration to immediately remove any and all remote access software from the computers of the Clerk-Treasurer's Office;

c. orders Mayor Cook and his Administration to remove any equipment from the Clerk-Treasurer's Office that is capable of audio recording;

d. enjoins Mayor Cook and his Administration from installing any software on the computers of the Clerk-Treasurer's Office without the express written permission of the Clerk-Treasurer;

e. enjoins Mayor Cook and his Administration from physically or electronically entering the Clerk-Treasurer's Office without the express permission of the Clerk-Treasurer; and

for all other relief as is just and proper in the premises.

Respectfully submitted,

/s/ Stephen W. Thompson
William J. Webster | No. 29086-29
Stephen W. Thompson | No. 29760-53
Danica L. Eyler | No. 24869-49
Attorneys for Plaintiff Cindy Gossard,
Clerk-Treasurer, City of Westfield, Indiana

COUNT II FOR DECLARATORY JUDGMENT

COMES NOW, Cindy Gossard, Clerk-Treasurer of the City of Westfield, Indiana, by counsel, and for Count II of her Complaint, states and alleges as follows:

81. Clerk-Treasurer Gossard incorporates, by reference, all preceding paragraphs of the present Complaint as if fully herein restated.

82. Pursuant to Indiana Code § 36-4-4-5, Clerk-Treasurer Gossard seeks declaration from the *en banc* Superior Court of Hamilton County that:

a. Clerk-Treasurer Gossard has the independent statutory authority to ensure the integrity and security of the financial systems, databases, and accounts maintained by the Clerk-Treasurer's Office;

b. Mayor Cook and his Administration does not have the statutory authority to monitor or interfere with the day to day operations of the Clerk-Treasurer's Office;

c. Mayor Cook does not have the statutory authority to access the computers of the Clerk Treasurer's Office without the Clerk-Treasurer's permission;

d. Mayor Cook does not have the statutory authority to conduct warrantless searches and seizures against the Clerk-Treasurer's Office; and

e. equipment located in the Clerk-Treasurer's Office is property belonging to and legally owned by the Clerk-Treasurer as an independent duly elected official of the City.

WHEREFORE, Cindy Gossard, Clerk-Treasurer of the City of Westfield, Indiana, respectfully requests that this Court issue declaratory judgment that:

a. Clerk-Treasurer Gossard has the independent statutory authority to ensure the integrity and security of the financial systems, databases, and accounts maintained by the Clerk-Treasurer's Office;

b. Mayor Cook and his Administration does not have the statutory authority to monitor or interfere with the day to day operations of the Clerk-Treasurer's Office;

c. Mayor Cook does not have the statutory authority to access the computers of the Clerk Treasurer's Office without the Clerk-Treasurer's permission;

d. Mayor Cook does not have the statutory authority to conduct warrantless searches and seizures against the Clerk-Treasurer's Office; and

e. equipment located in the Clerk-Treasurer's Office is property belonging to and legally owned by the Clerk-Treasurer as an independent duly elected official of the City.

for all other relief as is just and proper in the premises.

Respectfully submitted,

/s/ Stephen W. Thompson
William J. Webster ‖ No. 29086-29
Stephen W. Thompson ‖ No. 29760-53
Danica L. Eyler ‖ No. 24869-49
Attorneys for Plaintiff Cindy Gossard,
Clerk-Treasurer, City of Westfield, Indiana

Stephen W. Thompson, Esq.
WEBSTER & GARINO, LLC
115 N. Union Street
Westfield, IN 46074
Ph: 317/565-1818
Fax: 317/565-1835
sthompson@websterlegal.com

VERACITY
INTELLIGENCE•INVESTIGATION•RESEARCH

Prepared by:
Daniel Smith

VERACITY IIR
706 Pro-Med Ln #200a
Carmel, IN 46032317-925-1496

Report Date: September 1, 2021   INTERNAL CASE#: 99-2-414V

CLIENT:	Westfield Clerk Treasurer
ADDRESS:	130 Penn St. Westfield, IN 46074
PHONE:	(317) 804-3020

PRELIMINARY DIGITAL FORENSICS INVESTIGATION REPORT

SCOPE

On July 19, 2021 Veracity IIR was retained by Westfield Clerk Treasurer and requested to perform a digital forensic analysis of a computers used by Kimberly Strang, Beverly Rawlings, Debra Tolley, Cindy Gossard, Micha Farrer and Kerri Cagnon in order to ascertain if any software had been installed with the capacity to remotely monitor devices attached to the office network. Daniel Smith conducted all digital forensic responsibilities including forensic imaging, analysis and examination report drafting.

EXHIBIT
tabbies
1

Experience / Training

Daniel J. Smith
Digital Forensic Examiner

– Certified Computer Forensic Examiner –ACE Certified
– Certified Cellular Phone Forensic Examiner –ACE Certified
– Certified Talon Technician –Research Electronics International
– Technical Security Countermeasures 32 Hr. Course –TCC110 REI
– Digital Telephone Security Training 40 Hr. Course –DTC-210 REI
– Security+ (Plus) Certification (Core Network Security) – CompTia
– VSA Examiner (Voice Stress Analysis) – BMA Investigations

Experience

2017-Present All in Investigations, Inc,

– Cellular Forensics Examiner
– Computer Forensics Examiner
– Digital Data Forensics Examiner
– GPS Data Extractor
– GPS Data Analyzer
– Video Surveillance Installation Technician
– On-site Digital Security Systems Consulting
– Technical Surveillance Countermeasures Tech (TSCM)
– Court Appointed Digital Forensic Expert Witness

2006–2017 International Investigators Inc.

– 2011 Mobile Forensics World Guest Presenter: Blackberry Spyware Demo
– Field Surveillance Investigator
– Subpoena Process Server
– Cellular Forensic Examiner
– Computer Forensic Examiner
– GPS Data Extractor
– GPS Data Analyzer
– Video Surveillance Installation Tech

– On-site Security Systems Consulting
– Technical Surveillance Countermeasures Tech (TSCM)

Education

– 2004-2006 Purdue University
– Majored in Electrical Engineering at the School of Technology at Purdue University West Lafayette Campus

Advanced Training

– Mobil Forensics 101 –MFI
– Windows XP Forensics –MFI
– Windows Forensics Registry –MFI
– Call Detail Records and GPS Devices –MFI
– iPhone Forensics –MFI
– Mobile Phone Examiner –MFI
– Mobile Forensics –MFI
– AccessData Bootcamp –MFI
– TSCM –TALON –Telephone Analysis –REI
– Security + Certification –CompTia
– VSA Examiner –BMA Investigations

Forensic Imaging

Access to the Westfield Clerk Treasurer's offices was provided to the examiner by Clerk Treasurer Cindy Gossard on July 23, 2021 and again on July 26, 2021. Access to the office was provided by the Clerk Treasurer in order to forensically image the hard drives contained within the computers used by the office staff. The following devices were forensically imaged:

Below are the 8 forensically imaged hard drives involved in the examination:

- Desktop belonging to Cindy Gossard- Kingston SUV400S37-240G - WCTDT06
- Laptop belonging to Micha Farrer- SAMSUNG MZVLQ256HAJD-000H1 - WCTNB02
- Laptop belonging to Cindy Gossard - s/n: 5cd052qhc7 - WCTNB03

- Desktop belonging to Debra Tolley - MTFDHBA256TCK-1AS1AABHA - WITSPNB13
- Laptop belonging to Kimberly Strang - SSSTC CL1-8D256-HP - WCTNB04
- Desktop belonging to Kerri Cagnon - KINGSTON SV300S37A120G - WCTDT04
- Laptop belonging to Debra Tolley- SAMSUNG MZ7LN128HCHP-000 - WCTDT07
- Laptop belonging to Beverly Rawlings - SAMSUNG MZ7LN128HAHQ-000 (BitLocker Enabled)

NOTE: The above staff user accounts are labeled WDAGUtilityAccount in the ADF report.

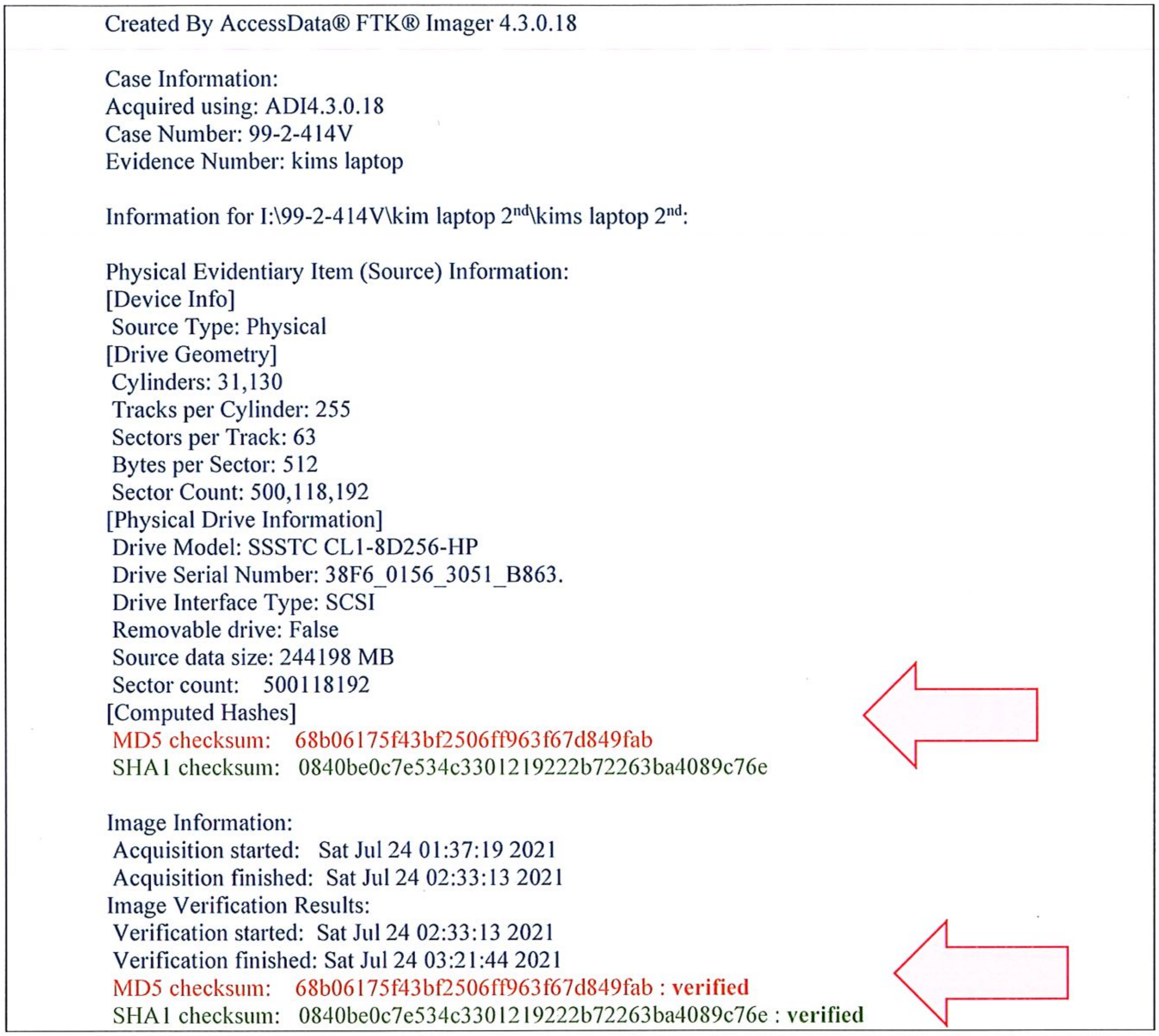
The Forensic Process

The forensic imaging process involves physically removing the hard drive from the target computer and then connecting the hard drive to a write blocker that prevents any data from being altered on the target hard drive during the imaging process. From the write blocker there is a connection via USB to the destination hard drive attached to a computer running the digital forensic software necessary to complete the forensic imaging. At no point during the imaging of the hard drives was any data accessed other than what was stored in the physical hard drive located in each target computer. Any network drives are temporarily detached automatically by the operating system once the target computers are turned off and hard drives removed for forensic imaging.

Forensic Software

Forensic Took Kit Imager 4.3 (FTK Imager) was used to create the images of the target hard drives. FTK Imager can create images in several formats however the E01 format was chosen in order to keep the image file sizes smaller via data compression as well as for the speed of the imaging process when utilizing the E01 format. Each target hard drive image was then verified by the calculated Hash value of the original data compared to the calculated Hash value of the forensic image created by FTK Imager.

Below is an example of the verification file created by FTK Imager for each hard drive.



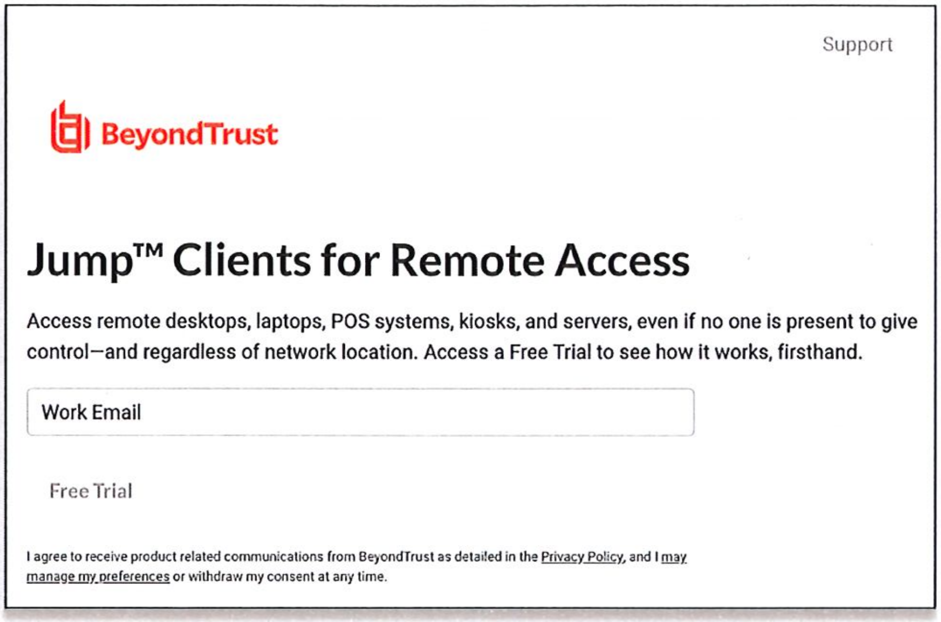
```
Created By AccessData® FTK® Imager 4.3.0.18

Case Information:
Acquired using: ADI4.3.0.18
Case Number: 99-2-414V
Evidence Number: kims laptop

Information for I:\99-2-414V\kim laptop 2nd\kims laptop 2nd:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 31,130
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 500,118,192
[Physical Drive Information]
 Drive Model: SSSTC CL1-8D256-HP
 Drive Serial Number: 38F6_0156_3051_B863.
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 244198 MB
 Sector count:    500118192
[Computed Hashes]
 MD5 checksum:    68b06175f43bf2506ff963f67d849fab
 SHA1 checksum:   0840be0c7e534c3301219222b72263ba4089c76e

Image Information:
 Acquisition started:   Sat Jul 24 01:37:19 2021
 Acquisition finished:  Sat Jul 24 02:33:13 2021
Image Verification Results:
 Verification started:  Sat Jul 24 02:33:13 2021
 Verification finished: Sat Jul 24 03:21:44 2021
 MD5 checksum:    68b06175f43bf2506ff963f67d849fab : verified
 SHA1 checksum:   0840be0c7e534c3301219222b72263ba4089c76e : verified
```

The image files were then analyzed by the examiner using ADF Digital Evidence Examiner PRO V2.3.3.133. Each image file was processed using a scanning function within the ADF software with priorities set to search for any evidence of remote network connections and if any were found then further attention was to be focused on the actions taken by such remote network connections.

Upon review of the scan results it was found that several anomalies were present within the imaged hard drives. There was a specific admin account named bgadmin and was found to have had remote access to nearly every device connected to the network in the office of the Westfield Clerk

Treasurer. Remote access software was found to have been installed by the bgadmin account including Papercut, Beyond Trust, and Jump Client for remote access.

Brief of software capabilities below as well as material taken directly from the software publishers websites describing some of the features of each.



Support

BeyondTrust

Jump™ Clients for Remote Access

Access remote desktops, laptops, POS systems, kiosks, and servers, even if no one is present to give control—and regardless of network location. Access a Free Trial to see how it works, firsthand.

Work Email

Free Trial

I agree to receive product related communications from BeyondTrust as detailed in the Privacy Policy, and I may manage my preferences or withdraw my consent at any time.

Figure 1 Beyond Trust: Jump Client for Remote Access has several features and capabilities. The Jump Client software in particular allows a user to remotely access data and local user actions without permission from the local user.

"Assist Any Remote Desktop, Server, or Mobile Device

Support all of your systems over the web, even if they are behind firewalls you don't control. All supported platforms are included in the core product, so you can consolidate and standardize support, improving incident handling time and support rep productivity.

BeyondTrust Remote Support works across Windows, Mac, Linux, Android, iOS, and Chrome OS. Access and control any remote computer or device, on-or-off the network—no VPN required. "

https://www.beyondtrust.com/remote-support

Excerpt above is from the Beyond Trust website

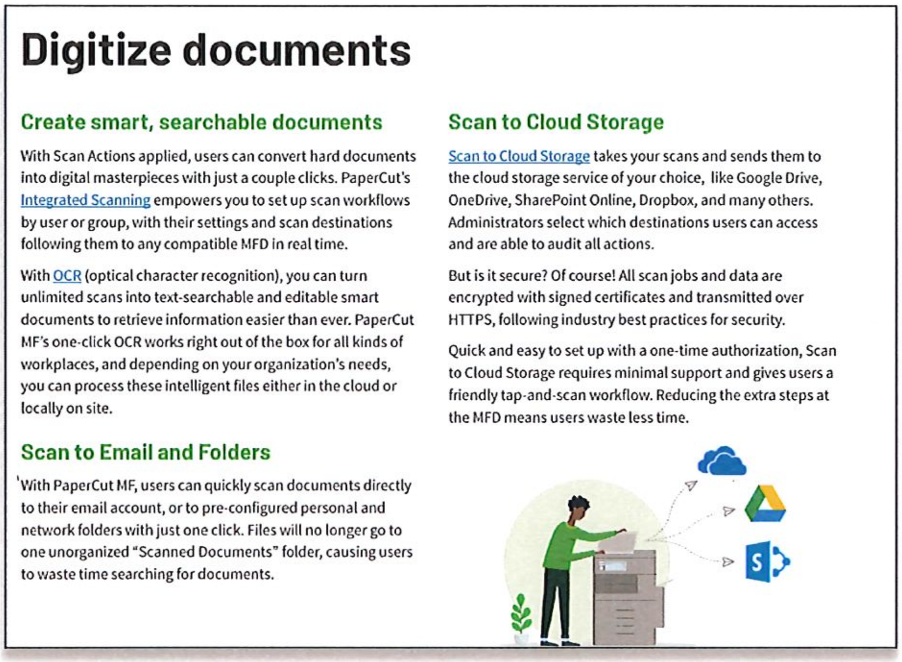
"Jump Clients let you control remote computers even when you don't control the remote network.

Simply install a Jump Client on each system you need to access and you'll be able to control it wherever it goes—without requiring the person on the other end of the session to be present."

https://www.beyondtrust.com/remote-support/features/jump-clients-remote-access

Excerpt above is from the Beyond Trust website

Beyond Trust software enables the user to see the remote clients computer screen as well as fully interact with the clients computer files and programs. The Jump Client feature was installed on all computers therefore allowing remote access to each computer without requiring the local user to be present. Since this software runs in the background the local user would not be aware their actions and data files were being accessed and/or observed by a remote user. The Beyond Trust software platform also can be used to control any network cameras and microphones including the built in microphones and cameras on laptops without the local users knowledge.



Digitize documents

Create smart, searchable documents

With Scan Actions applied, users can convert hard documents into digital masterpieces with just a couple clicks. PaperCut's Integrated Scanning empowers you to set up scan workflows by user or group, with their settings and scan destinations following them to any compatible MFD in real time.

With OCR (optical character recognition), you can turn unlimited scans into text-searchable and editable smart documents to retrieve information easier than ever. PaperCut MF's one-click OCR works right out of the box for all kinds of workplaces, and depending on your organization's needs, you can process these intelligent files either in the cloud or locally on site.

Scan to Email and Folders

With PaperCut MF, users can quickly scan documents directly to their email account, or to pre-configured personal and network folders with just one click. Files will no longer go to one unorganized "Scanned Documents" folder, causing users to waste time searching for documents.

Scan to Cloud Storage

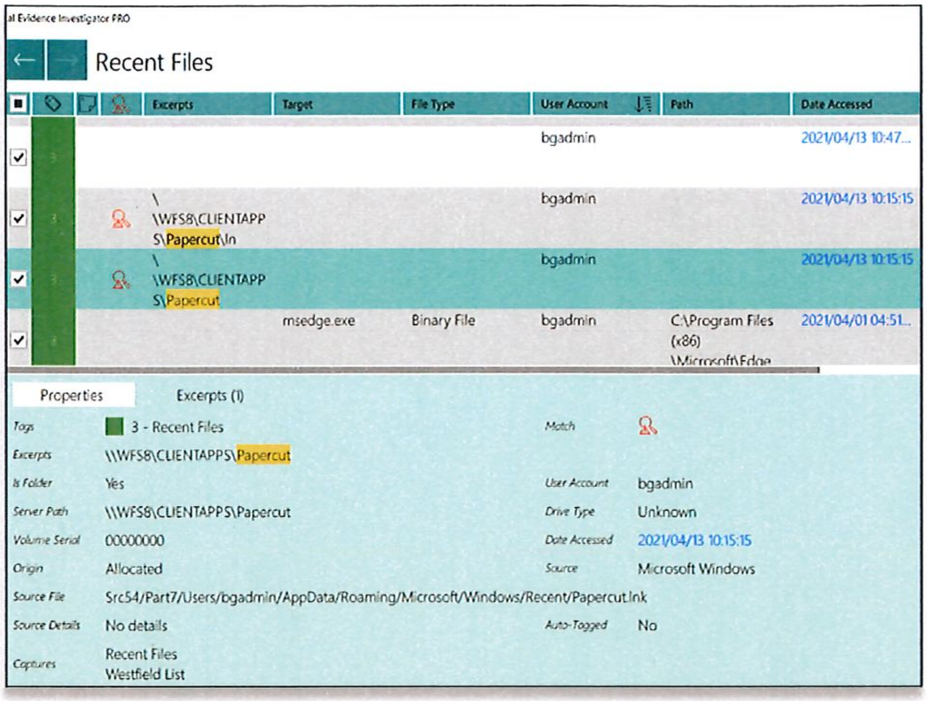
Scan to Cloud Storage takes your scans and sends them to the cloud storage service of your choice, like Google Drive, OneDrive, SharePoint Online, Dropbox, and many others. Administrators select which destinations users can access and are able to audit all actions.

But is it secure? Of course! All scan jobs and data are encrypted with signed certificates and transmitted over HTTPS, following industry best practices for security.

Quick and easy to set up with a one-time authorization, Scan to Cloud Storage requires minimal support and gives users a friendly tap-and-scan workflow. Reducing the extra steps at the MFD means users waste less time.

Figure 2. Papercut software has capabilities such as the feature that allows a remote user the ability to see any document that has been scanned, copied or printed from any local user on the network. The above excerpt was retrieved from the Papercut website (www.papercut.com).

Papercut software was discovered being used by two different user accounts bgadmin and Informatics with the majority of the software's use coming from the bgadmin user account. Papercut allows the remote admin to access digital copies of scanned and printed documents. If the WCT staff was unaware of this program it is possible sensitive information could have been observed by whomever was operating the remote user accounts with access to the papercut web portal.



al Evidence Investigator PRO

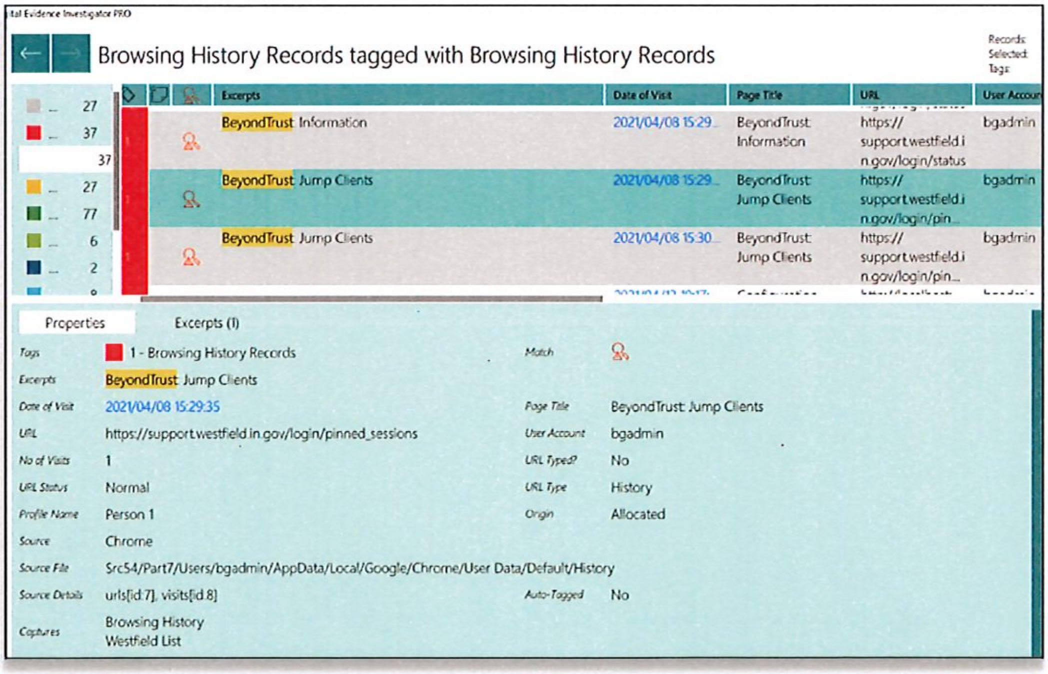
Recent Files

■				Excerpts	Target	File Type	User Account	Path	Date Accessed
☑	3						bgadmin		2021/04/13 10:47...
☑	3			\ \WFS8\CLIENTAPP S\Papercut\In			bgadmin		2021/04/13 10:15:15
☑	3			\ \WFS8\CLIENTAPP S\Papercut			bgadmin		2021/04/13 10:15:15
☑	3				msedge.exe	Binary File	bgadmin	C:\Program Files (x86) \Microsoft\Edge	2021/04/01 04:51...

Properties   Excerpts (1)

Tags	🟩 3 - Recent Files	Match	
Excerpts	\\WFS8\CLIENTAPPS\Papercut		
Is Folder	Yes	User Account	bgadmin
Server Path	\\WFS8\CLIENTAPPS\Papercut	Drive Type	Unknown
Volume Serial	00000000	Date Accessed	2021/04/13 10:15:15
Origin	Allocated	Source	Microsoft Windows
Source File	Src54/Part7/Users/bgadmin/AppData/Roaming/Microsoft/Windows/Recent/Papercut.lnk		
Source Details	No details	Auto-Tagged	No
Captures	Recent Files Westfield List		

Figure 3. A screen grab of evidence from ADF Digital Evidence Investigator software showing bgadmin (profile "Person 1") utilizing the Papercut software remotely on the Westfield Clerk Treasurer's Cindy Gossard's laptop.



tal Evidence Investigator PRO

Browsing History Records tagged with Browsing History Records

Records:
Selected:
Tags:

...	27
🟥 ...	37
	37
🟧 ...	27
🟩 ...	77
🟩 ...	6
🟦 ...	2

			Excerpts	Date of Visit	Page Title	URL	User Accoun
1			BeyondTrust Information	2021/04/08 15:29...	BeyondTrust Information	https:// support.westfield.i n.gov/login/status	bgadmin
1			BeyondTrust Jump Clients	2021/04/08 15:29...	BeyondTrust Jump Clients	https:// support.westfield.i n.gov/login/pin...	bgadmin
1			BeyondTrust Jump Clients	2021/04/08 15:30...	BeyondTrust Jump Clients	https:// support.westfield.i n.gov/login/pin...	bgadmin

Properties   Excerpts (1)

Tags	🟥 1 - Browsing History Records	Match	
Excerpts	BeyondTrust Jump Clients		
Date of Visit	2021/04/08 15:29:35	Page Title	BeyondTrust Jump Clients
URL	https://support.westfield.in.gov/login/pinned_sessions	User Account	bgadmin
No of Visits	1	URL Typed?	No
URL Status	Normal	URL Type	History
Profile Name	Person 1	Origin	Allocated
Source	Chrome		
Source File	Src54/Part7/Users/bgadmin/AppData/Local/Google/Chrome/User Data/Default/History		
Source Details	urls[id:7], visits[id:8]	Auto-Tagged	No
Captures	Browsing History Westfield List		

Figure 4. An example of evidence ADF Digital Evidence Investigator software showing bgadmin (profile "Person 1") utilizing the Beyond Trust Jump Client software remotely on Westfield Clerk Treasurer's Cindy Gossard's laptop.

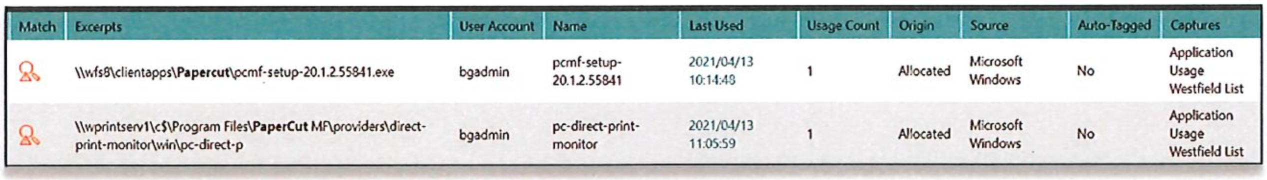
At the time of this report access to Beverly Rawlings hard drive data was limited due to the enabled BitLocker encryption. This encryption requires a BitLocker key to decrypt so that the hard drive data can be accessed. If the BitLocker key was provided then access to the imaged hard drive data would be possible.

More time is required in order to examine all of the hard drives more thoroughly but after a preliminary examination the following was discovered:

- **3609** files were access, altered or created by the user account bgadmin during remote access sessions to the office computers of the Westfield Clerk Treasurer's office. This url link used in many of these sessions pointed to the Beyond Trust web portal using the following address: https://support.westfield.in.gov/. The majority of these files were found to have been accessed between December 2020 and April 2021.

- Remote Support Jump Client 20.1.1 was found installed on all 7 hard drives examined and were installed by user account bgadmin. This is a product by Beyond Trust and does not require the local user on the targeted computer to give permission to the remote network connection. Furthermore, Beyond Trust software does not make the local user aware that the remote access session has ever started nor ended.

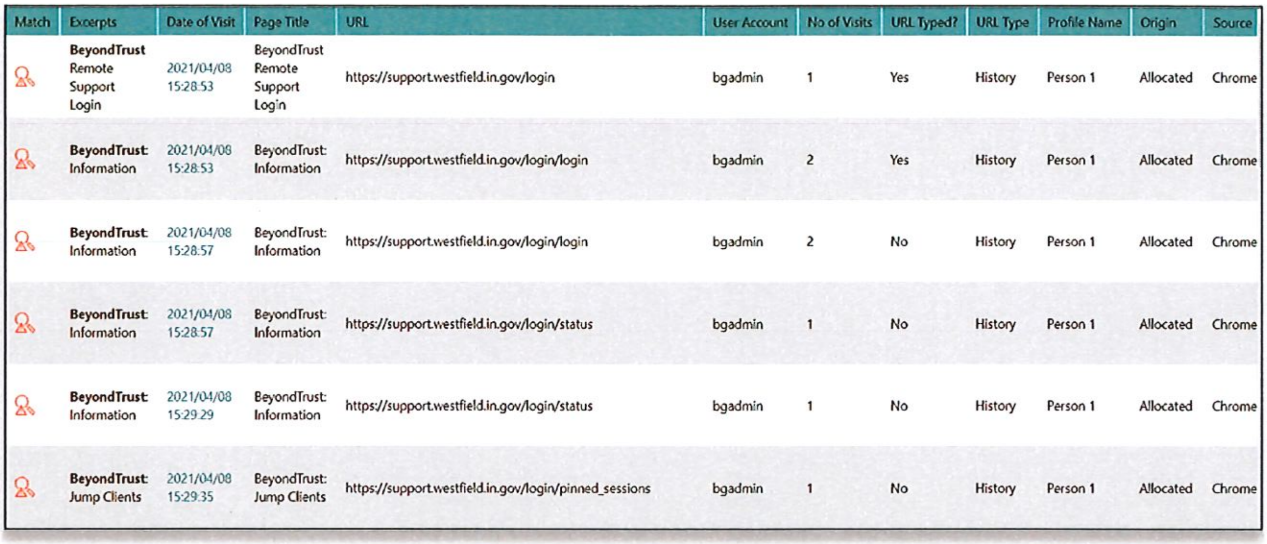
- On April 13, 2021 at 10:14am user account bgadmin used the software Papercut and again at 11:05am to access documents that had either been scanned, printed or copied from the printer in the WCT office. The following figure shows details obtained from these occurrences. The user account bgadmin had other instances of using the Papercut software as included in the



Match	Excerpts	User Account	Name	Last Used	Usage Count	Origin	Source	Auto-Tagged	Captures
🔍	\\wfs8\clientapps\Papercut\pcmf-setup-20.1.2.55841.exe	bgadmin	pcmf-setup-20.1.2.55841	2021/04/13 10:14:48	1	Allocated	Microsoft Windows	No	Application Usage Westfield List
🔍	\\wprintserv1\c$\Program Files**PaperCut** MF\providers\direct-print-monitor\win\pc-direct-p	bgadmin	pc-direct-print-monitor	2021/04/13 11:05:59	1	Allocated	Microsoft Windows	No	Application Usage Westfield List

Figure 5. Details obtained from user bgadmin usage of Papercut software.

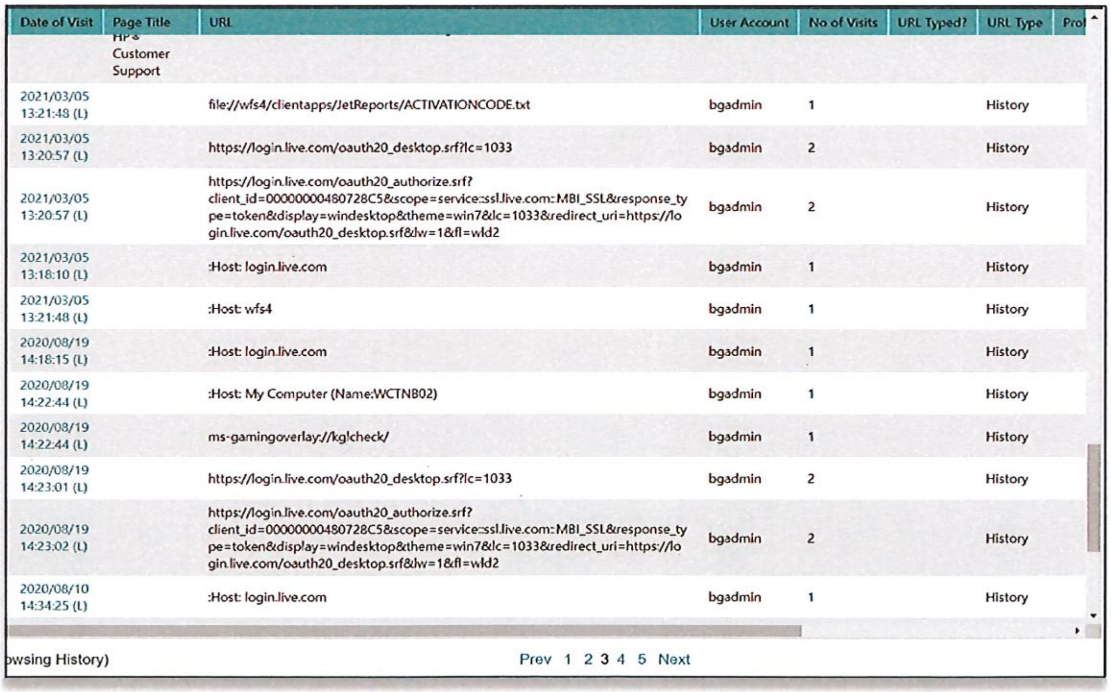
- **At least 35** separate remote sessions were found to have been conducted by user bgadmin using Beyond Trust software on the Westfield Clerk Treasurer's office computers with the first known usage starting on March 15, 2020. The following figure shows details obtained from several of these occurrences.



Match	Excerpts	Date of Visit	Page Title	URL	User Account	No of Visits	URL Typed?	URL Type	Profile Name	Origin	Source
	BeyondTrust Remote Support Login	2021/04/08 15:28:53	BeyondTrust Remote Support Login	https://support.westfield.in.gov/login	bgadmin	1	Yes	History	Person 1	Allocated	Chrome
	BeyondTrust: Information	2021/04/08 15:28:53	BeyondTrust: Information	https://support.westfield.in.gov/login/login	bgadmin	2	Yes	History	Person 1	Allocated	Chrome
	BeyondTrust: Information	2021/04/08 15:28:57	BeyondTrust: Information	https://support.westfield.in.gov/login/login	bgadmin	2	No	History	Person 1	Allocated	Chrome
	BeyondTrust: Information	2021/04/08 15:28:57	BeyondTrust: Information	https://support.westfield.in.gov/login/status	bgadmin	1	No	History	Person 1	Allocated	Chrome
	BeyondTrust: Information	2021/04/08 15:29:29	BeyondTrust: Information	https://support.westfield.in.gov/login/status	bgadmin	1	No	History	Person 1	Allocated	Chrome
	BeyondTrust: Jump Clients	2021/04/08 15:29:35	BeyondTrust: Jump Clients	https://support.westfield.in.gov/login/pinned_sessions	bgadmin	1	No	History	Person 1	Allocated	Chrome

Figure 6. Details obtained from several occurrences of user bgadmin using Beyond Trust software on the office computers at the Westfield Clerk Treasurer.

- **220** occurrences of user bgadmin network artifacts were obtained from Westfield Clerk Treasurer office computers. These were actions taken on the local office computers by the remote user bgadmin.



Date of Visit	Page Title	URL	User Account	No of Visits	URL Typed?	URL Type	Prof
	HP's Customer Support						
2021/03/05 13:21:48 (L)		file://wfs4/clientapps/JetReports/ACTIVATIONCODE.txt	bgadmin	1		History	
2021/03/05 13:20:57 (L)		https://login.live.com/oauth20_desktop.srf?lc=1033	bgadmin	2		History	
2021/03/05 13:20:57 (L)		https://login.live.com/oauth20_authorize.srf?client_id=00000000480728C5&scope=service::ssl.live.com::MBI_SSL&response_type=token&display=windesktop&theme=win7&lc=1033&redirect_uri=https://login.live.com/oauth20_desktop.srf&lw=1&fl=wld2	bgadmin	2		History	
2021/03/05 13:18:10 (L)		:Host: login.live.com	bgadmin	1		History	
2021/03/05 13:21:48 (L)		:Host: wfs4	bgadmin	1		History	
2020/08/19 14:18:15 (L)		:Host: login.live.com	bgadmin	1		History	
2020/08/19 14:22:44 (L)		:Host: My Computer (Name:WCTNB02)	bgadmin	1		History	
2020/08/19 14:22:44 (L)		ms-gamingoverlay://kg!check/	bgadmin	1		History	
2020/08/19 14:23:01 (L)		https://login.live.com/oauth20_desktop.srf?lc=1033	bgadmin	2		History	
2020/08/19 14:23:02 (L)		https://login.live.com/oauth20_authorize.srf?client_id=00000000480728C5&scope=service::ssl.live.com::MBI_SSL&response_type=token&display=windesktop&theme=win7&lc=1033&redirect_uri=https://login.live.com/oauth20_desktop.srf&lw=1&fl=wld2	bgadmin	2		History	
2020/08/10 14:34:25 (L)		:Host: login.live.com	bgadmin	1		History	

Figure 7. Example from ADF Digital Evidence Investigator illustrating artifacts obtained from web browser history events.

- **198** file records associated with Beyond Trust software and user bgadmin were obtained in the initial examination of the WCT office hard drives. These records included appcache type files which were developed initially to let web applications run offline, no internet connection required, but can also be used online to decrease application load times.

- There were **2** discovered incidents of user Informatics remotely using the software Papercut on offices in the WCT. No evidence was found of Beyond Trust or Papercut software being used by any of the office staff user accounts.

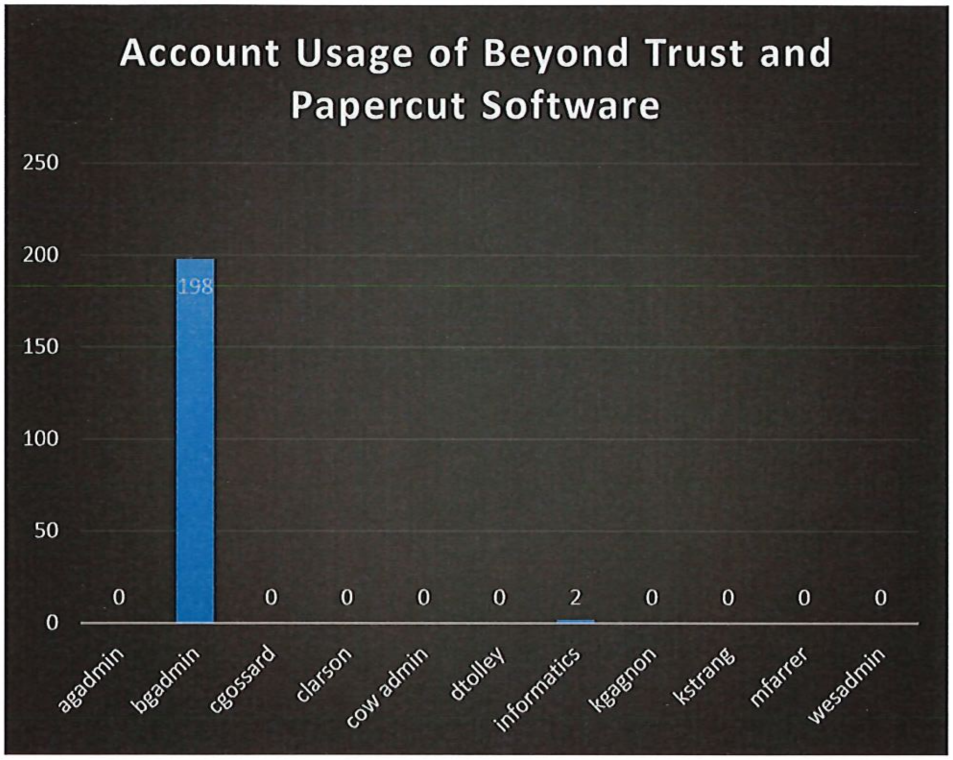
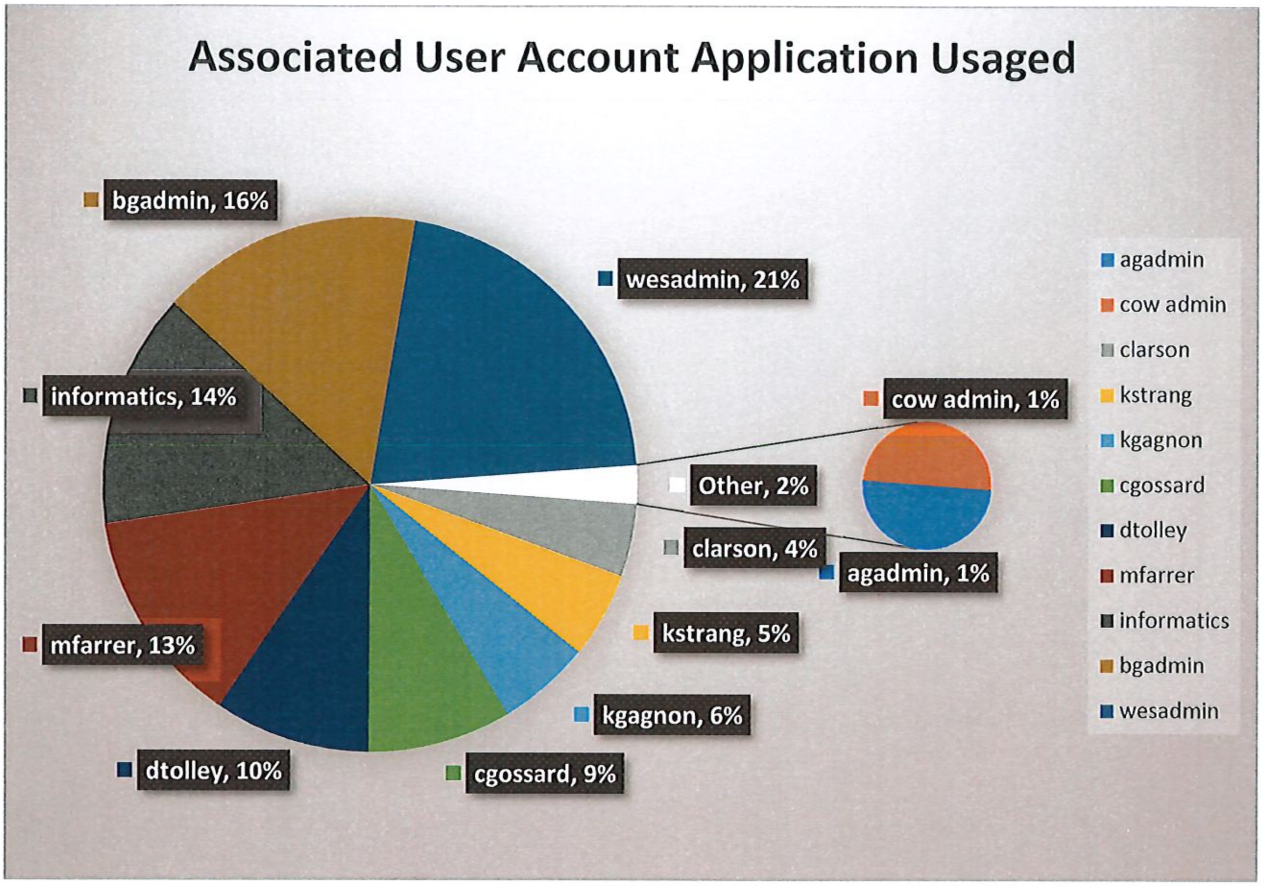


Figure 8. The above graph illustrates the disparity in use of remote access software Beyond Trust and Papercut. Neither software requires the local user to give permission for a remote session. 99% of Beyond Trust and Papercut software use was from the bgadmin account and the remaining 1% was from the Informatics account. There was no evidence found of any other accounts using either of these remote access software platforms.

- **1517** timeline events were extracted that were associated with user bgadmin. These events included remote access to files in the WCT office computers, application uses, files created/modified, browser usage, Papercut software usage, as well as others. Timeline events are timestamped events logged by the local computers operating system.

In the chart below shows the normal deviation of application usage from all accounts from all applications installed on the computers. The bgadmin account used 16% of the overall obtained application usage records, however, as shown in the graph above the bgadmin account was involved with 99% of all discovered application uses of Beyond Trust and Papercut.



Anomalies requiring further investigation

From the evidence investigated at this point it is unclear why the bgadmin account was primarily involved with the use of Beyond Trust, Jump Client and Papercut software. It appears that the Informatics account would have been fully capable of using the above previously mentioned software platforms and was an account that the WCT office staff was aware of. It is assumed that with more time to complete the forensic evaluation it could be revealed why the bgadmin account was hidden from the WCT office staff as well as the question as to why it appears the main use of this account was to use remote access programs capable of observing and even saving screen shots, file records and other activities of the local users. Informatics was already being used as a remote IT administration account and should have been able to handle any remote access responsibilities with the already installed Microsoft Zoom and Team Viewer software which could have also required the WCT office staff to willfully allow permission to access their local computer.

Further analysis must also be conducted on evidence of a possible password breaking software being used remotely on the local accounts. Several pieces of evidence included what appears to be tables created by software for the explicit use of attacking unknown passwords on the local computers. Tables are merely files that contain huge amounts of words, either randomly created by an algorithm or captured via user input, in order to be used by a password breaking program for the purpose of hacking unknown passwords. Appcache data was found with a strong indication that Beyond Trust was connected with the text files appearing to be password hacking tables. Beyond Trust has software called Vault that has the capability to use a built-in discovery tool to scan and import Active Directory as well as local accounts in order to attempt password/credential access.

END PRELIMINARY DIGITAL FORENSIC INVESTIGATION REPORT