Data Security Assessment: Complete Genomics' US Customer Offering

PUBLISHED OCTOBER 18, 2023

FTI Cybersecurity

An Intelligence-Led, Expert-Driven, Strategic Approach to
Global Cybersecurity Challenges

Prepared for COMPLETE GENOMICS

The information contained in this report is strictly confidential and intended only for the use of the individual or entity to which it is addressed.
This report may not be copied, distributed, or disclosed to any other individual or entity whatsoever.

Table of Contents

1. EXECUTIVE SUMMARY

FTI Consulting, Inc. ("FTI") was engaged by Complete Genomics ("Client" or "CG") to conduct network monitoring, vulnerability assessments, and hardware and source code review pertaining to its DNBSEQ-T7 product ("T7"), sold to US customers as a package that additionally includes a separate Linux based Server ("ZTRON Lite" or "ZTRON") used for storing, processing, and transmitting genomic sequencing data produced by the T7, between August 30, 2023 and October 16, 2023.[1] This assessment sought to identify the existence and nature of any outbound network traffic occurring during US customers' expected DNA sequencing operations while using the T7 and ZTRON.

1.1 Key Findings

1.1.1 Network Capture

Live network captures from the ZTRON server revealed external Internet Protocol (IP) activity and traffic attributable to known Linux repositories, Domain Name System (DNS), and Network Time Protocol (NTP) servers (collectively "system functionality IPs") which were all based in the United States of America and considered expected traffic.

Further analysis of the system functionality IPs revealed no meaningful data transfer in the outbound traffic.

1.1.2 Software Source Code Review

Results from review of limited[2] ZTRON source code indicated that the domain name "ztron.mgi-tech.com" is hardcoded within the code for the apparent purpose to access and transfer data. According to information from CG, this functionality is intended for the global version of the ZTRON's operating system only. This statement is consistent with FTI's observations that the ZTRON's US version operating system did not appear to invoke this functionality, as the IP address corresponding to that domain did not appear in network captures.

1.1.3 Vulnerability Scans

FTI conducted vulnerability scans on three (3) systems, to include the ZTRON, as well as two Windows 10 operating systems, which are part of the T7, and which are described in further detail later in this report. FTI identified vulnerabilities on all three systems, ranging in criticality from industry accepted tooling categories 'critical' to 'informational'.[3]

[1] CG maintains multiple versions of its ZTRON operating system, such as for US customers and non-US customers, as well as multiple versions of its source code base. This report covers the US version of the ZTRON operating system and source code.

[2] Only code related to data communications on the ZTRON was considered in review scope.

[3] https://docs.tenable.com/nessus/Content/RiskMetrics.htm

The effective criticality of the identified vulnerabilities, however, depends on the system context.[4] For this reason, FTI recommends that CG review the vulnerabilities in full and within context, though FTI does not have immediate reason to believe that any of the identified vulnerabilities 1) pose a significant threat to the legitimacy or efficacy of FTI's testing procedures; 2) have any connection to the external IP connections that were made during regular operations of the systems; or 3) pose an apparent threat to the security of the ZTRON as delivered to US clients.

1.1.4 Hardware Schematic Review

FTI identified no inconsistencies in the hardware schematic design, design rules, schematic conventions, and documentation related to the ZTRON. FTI assesses that CG's schematic diagrams are of a high-quality design and engineering work product.

1.2 Disclaimers

FTI notes that all network traffic was captured on CG configured devices and within a CG controlled environment. Additionally, all software repositories and resources were provided by CG under the assumption that it accurately reflects the live CG software repositories; the software environment that FTI accessed was fully controlled and managed by CG personnel.

Finally, given the volume of data produced in the genetic sequencing process, FTI made judgement calls to arrive at its selected sample sizes used for the network monitoring component. These judgement calls are described in the detailed findings section of this report.

2. SYSTEM BACKGROUND

On August 30, 2023, FTI participated in informational sessions, including tours of the facility, machinery, and code, led by the following points of contact at CG:

1. **Maxim Hudaley**, Project Manager for this project and main point of contact.
    - Email: mhudaley@completegenomics.com
    - Phone: 408.438.8715
2. **Biniam Feleke**, Devices functions, configuration, and operation.
    - Email: bfeleke@completegenomics.com
    - Phone: 608.695.3817
3. **Yizhe Jason Zhang**, Software.
    - Email: yzhang@completegenomics.com
    - Phone: 651.235.6276
4. **Logan Schiller**, Lab.
    - Email: lschiller@completegenomics.com

[4] For example, the same vulnerability may pose a more significant threat if the system is configured on a vulnerable network versus an air gapped network (which is not internet-connected).

- Phone: 925.989.9225

Through these conversations and facility observations, FTI identified the following:

2.1.1 T7 Design and Function Overview

The T7 is a DNA sequencing machine that provides comprehensive DNA analysis for clients in medicine and research among other fields. It works by receiving up to three prepared Nanoball Trays (DNB), fed into the machine itself. Inside the casing of the T7 are two computing functions – one controlling the machine's mechanical operations ("BCS"), and a second ("SBC") controlling the flow of sequencing data generated by the T7 and sent to the ZTRON storage server. Both computers inside the T7 run the Windows 10 Operating System ("Win 10 OS").

The SBC Win 10 OS is accessible via a display screen on the front of the T7 while The BCS Win 10 OS is available via remote access from the SBC Win 10 OS, or through a remote session enabled by a direct ethernet connection. Both computers have corresponding ethernet connections. Among the accessible input and output ("I/O") is a blue fiber wire, responsible for high throughput transmission of data from the T7 to the ZTRON server, responsible for processing, storing, and – depending on client preference – sending the data received from the T7 elsewhere.

See Appendix B for detailed photos on the T7.

2.1.2 ZTRON Design and Function Overview

The ZTRON server runs Linux CentoOS 7 as its operating system. CG has made approximately four updates to its ZTRON's CentOS 7 configuration over the last five years. Though technically different machines, CG's US-based customers have only ever purchased both the T7 and ZTRON as a package, according to CG, given that CG configures the ZTRON OS for out-of-the-box operation, and which a client can use almost immediately with minimal configuration. A client can thereafter choose a different setup environment if desired, such as using an internet connection to send the data from the ZTRON to cloud storage or configuring internal networking to a local storage server separate from the ZTRON. These types of setups may be chosen to, for example, free up space on the ZTRON or serve as a backup solution. The ZTRON can accommodate such client preferred scenarios, and CG offers the client's IT department support in making these initial configurations, but strongly advises against additional configuration changes thereafter given the complexities involved.

The sequencing data generated by the T7 is sent to the ZTRON through the fiber connection, chosen due to its ability for high data throughout. Once the data is on the ZTRON, it can be sent out through another fiber connection. The ZTRON may also be connected to Wi-Fi or ethernet, and can send data via those methods instead of fiber, if chosen by the customer.

The data flow, per conversations with CG and confirmed by FTI's observations of network traffic discussed in more detail later in this report, is unidirectional. That is, the sequencing data flows only one way from the T7 to the ZTRON. While there is an option to encrypt data from the T7, CG did not have the option enabled on the machines provided for testing, as confirmed by Mr. Schiller after consultation with the corporate bioinformatics manager.

See Appendix C for detailed photos on the ZTRON.

3. DETAILED FINDINGS

At intervals spanning August 31, 2023 through October 9, 2023, FTI conducted live capturing of network traffic during normal operating use of the T7 and ZTRON systems. Once network traffic captures were completed, FTI conducted analysis on this data to understand what, if any, external IP addresses were contacted during normal use.

In addition to network traffic analysis, FTI conducted a static source code review of select CG software repositories related to data communication, conducted vulnerability scans on the ZTRON and T7, and reviewed hardware schematics. Each of these workstreams is discussed in further detail in this section.

3.1 Methodology

3.1.1 Network Capture

FTI chose to capture the network traffic at the point of the ZTRON, and not on the T7, because no US customer has purchased the T7 without the ZTRON. Specifically, while the T7 could be configured for internet connectivity, it has not been sold in such a configuration within the US, according to CG. As such, the ZTRON serves as the machine closet to internet connectivity, if a US client chooses to utilize internet connectivity at all, as discussed in the ZTRON Design and Function Overview above.[5] FTI further decided on a 24x7 (24 hours a day for approximately 7 days) network capture to balance the volume of data produced with sufficient time for observation of traffic under varying conditions, to include active sequencing job processing, system at rest, and with internet connected and disconnected.

On October 2, 2023, in conducting its primary 24x7 capture on the ZTRON, FTI used a Verizon hotspot, connected to the ZTRON server via ethernet to provide internet connectivity separate from CG's network. To do so, FTI temporarily turned off the 802.1x security option[6], which it reenabled on October 6, 2023. Altogether, FTI's network collections on the ZTRON included internet connectivity

[5] For this reason, further scoping could include conducting an additional physical network tab on the fiber connection between the two devices.

[6] 802.1X security is the name of the IEEE standard for port-based Network Access Control (PNAC). It is also called WPA Enterprise. 802.1X security is a way of controlling access to a logical network from a physical one. All clients who want to join the logical network must authenticate with the server (a router, for example) using the correct 802.1X authentication method. This setting was turned off in order to allow a simpler connection to the Verizon hotspot.

traffic from October 2 – October 6, 2023 and no internet connectivity from October 6 – October 9, 2023. During this time period, CG ran a sequencing job beginning approximately 5pm PDT October 3 and running to approximately 1am PDT October 4, 2023. Upon completion of its network capture, FTI collected approximately 1.8TB of network activity, stored on an external 8TB drive that FTI had connected to the ZTRON. This data was then copied to a 8TB Western Digital backup drive, on which FTI conducted its processing and analysis.

On August 31, 2023, FTI additionally captured approximately 20 minutes of packets from both the BCS and SBS machines in the T7 for a preliminary sample analysis.

3.1.2 Software Source Code Review

FTI arranged with CG to allow for remote access to a limited portion of the software that is related to data communication. To conduct this review without providing a copy of the code, CG arranged for an on-site laptop to which FTI could remote into via virtual private network (VPN), and which contained appropriate software analysis tooling. CG used a controlled sandbox environment, and the devices used a mix of C#, C++, Java, SQL, and Veralog.

On October 2, 2023, FTI used the open-source tool, Gitleaks[7], to conduct a preliminary test of any hardcoded, sensitive information that exists in the source code and parent directories. Gitleaks flagged several files, which were subsequently manually reviewed to eliminate false positives and obtain a holistic understanding of the context and purpose of the code in which the identified vulnerabilities existed. Regular expression (“regex”) commands were also implemented to recursively search the “Z:\MGI” directory and its subdirectories for any hardcoded IP addresses and domain names.

3.1.3 Vulnerability Scans

During FTI’s inspection and analysis of CG devices, FTI conducted a set of vulnerability scans across all accessible components of the in-scope sequencing devices.

On August 31, 2023 and October 2, 2023, FTI used Nessus Professional to conduct a basic scan limited to common ports, so as to conduct the most stable scan in CG’s production environment. To conduct this scan of the T7 Windows operating systems on August 31, 2023, FTI created a private subnet using a NetGear router to which the respective T7 Windows Operating Systems were connected via ethernet. Additionally, on October 2, 2023, FTI used a Verizon hotspot to create a Local Area Network (“LAN”) which was used to conduct its scans of the ZTRON. See Appendix D for detailed photos.

[7] See more information in the Gitleaks repository: https://github.com/gitleaks/gitleaks

3.2 Analysis

3.2.1 Network Capture

FTI conducted its analysis on the captured 1.8TB of network data to identify whether connections with external IP addresses were being made. FTI began by processing the captured data which was in the form of packet capture (pcap) data using TShark[8] to filter out all private IP addresses which are used within the internal network. FTI notes that throughout analysis, both commonly used internal IP ranges as well as custom internal ranges were filtered out of the larger network traffic data. CG was able to confirm that the network range of 198.17.238.0/24 was used by locally hosted applications, which comprised a large portion of network traffic, and thus could be filtered out. FTI's full TShark command can be found below which depicts the network ranges that were excluded from analysis.

```
tshark -r "$pcap_file" -Y "ip.dst !== 192.168.0.0/16 and ip.dst !== 172.16.0.0/12 and ip.dst !==
10.0.0.0/8 and ip.dst !== 127.0.0.0/8 and ip.dst !== 169.254.0.0/16 ip.dst !== 198.17.238.0/24 and not
(ip.dst in {224.0.0.251, 239.255.255.250, 239.255.255.253, 198.18.0.0/15})" -w - -B 9000000
```

After filtering out internal IP traffic, FTI identified that connections were established with approximately 46 unique external IP addresses listed in Appendix A, during the ZTRON's operating use.

Next, analysts queried each of the 46 external IP addresses via relevant domain lookup tools. From this effort, FTI mapped domain names to each IP address, observing that some IP addresses resolve to multiple domain names.

IPs identified as part of typical Linux system operation

Domain mapping revealed many of the IP addresses resolved to known domains associated with normal, or expected, activities related to the CentOS operating system in use by the ZTRON. Specifically, FTI analysts collected a list of the known CentOS domains known as "Mirrors" from the official CentOS website[9] on September 21, 2023. A Linux mirror, in the context of software repositories, is a server or network of servers that store copies of a Linux distribution's software packages, libraries, and updates. These mirrors allow users to download software and updates from geographically distributed sources, enhancing the availability and speed of software distribution for Linux users.

Fedora and CentOS are closely related Linux distributions that originate from the same upstream vendor, Red Hat. In further research, FTI identified additional domain names that were attributable to

[8] TShark is a network protocol analyzer. It lets a user capture packet data from a live network, or read packets from a previously saved capture file.

[9] https://www.centos.org/download/mirrors/

Fedora Linux mirror infrastructure,[10] which can occur when shared common dependencies or libraries exist. That is, if an application or package on a CentOS system requires a library or package that is not available in CentOS repositories, the package manager may try to resolve the dependencies by looking in other repositories, including Fedora mirrors. To this end, FTI was also able to attribute additional IP addresses to the Extra Packages for Enterprise Linux ("EPEL") repository.[11] FTI notes that CentOS, Fedora, and EPEL all fall under the general Fedora Linux project – a well-known and popular Linux distribution.

The purpose for ZTRON establishing network connections with these non-Fedora mirrors could be due to library or dependencies that exist elsewhere or custom package manager mirror configuration, and this traffic would typically occur under normal Linux operating system conditions.

Using WireShark,[12] FTI conducted further analysis on various samples of packet capture data to more closely analyze the network traffic that was occurring to the identified IP addresses. Throughout its analysis, FTI found that all network traffic to and from external IPs that were contacted were related to basic Linux behavior and did not contain any meaningful data. Instead, the traffic either related to Domain Name System ("DNS") queries to DNS servers, contact with a Network Time Protocol ("NTP") server, used to sync system clocks, or were part of a TCP handshake[13], and which did not appear to transmit any additional data with the external IP upon completion of the handshake.[14] The below IP addresses communicated with the ZTRON relating to NTP data.

Figure 4 – External IP Addresses Attributable to NTP Servers

IP Address	Country of Origin
204.93.207.12	United States
209.51.161.238	United States
66.228.59.187	United States
165.140.142.118	United States
74.207.242.234	United States
216.229.0.50	United States

[10] https://admin.fedoraproject.org/mirrormanager/mirrors/Fedora

[11] https://admin.fedoraproject.org/mirrormanager/mirrors/EPEL

[12] WireShark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

[13] TCP is a stateful protocol between client and server that involves a sequence of packet data back and forth in order to establish a connection

[14] An established TCP connection can be used to transmit and receive data, however throughout FTI's analysis, these connections were not seen to have been used for data transfer, and instead indicate normal Linux operating system behavior such as ensuring a strong connection to a Linux mirror.

44.190.5.123	United States
151.204.223.236	United States

Additional IP analysis can be found in Appendix A.

Analysis of BCS and SBC network captures

FTI also conducted a capture of approximately 20 minutes of traffic from the BCS and SBC windows machines by using “netsh trace”, a built-in windows tool that can be used to capture network traffic. The output of this tool results in .cab and .etl files, which can be converted to a readable pcap file using the tool “etl2pcapng.exe”[15], an open-sourced tool developed by Microsoft employees to replace a deprecated Microsoft tool.

In analyzing the converted .etl file in WireShark, FTI was able to filter out any private (non-externally routable) IP addresses and was left with no meaningful results. The Wireshark command that was used can be found below:

```
!ip.addr == 192.168.0.0/16 && !ip.addr == 172.16.0.0/12 && !ip.addr == 10.0.0.0/8
```

These findings align with FTI’s understanding that the BCS and SBC devices are not connected to any internet networks, meaning that they are unable to establish network traffic with any external IP addresses.

3.2.2 Software Source Code Review

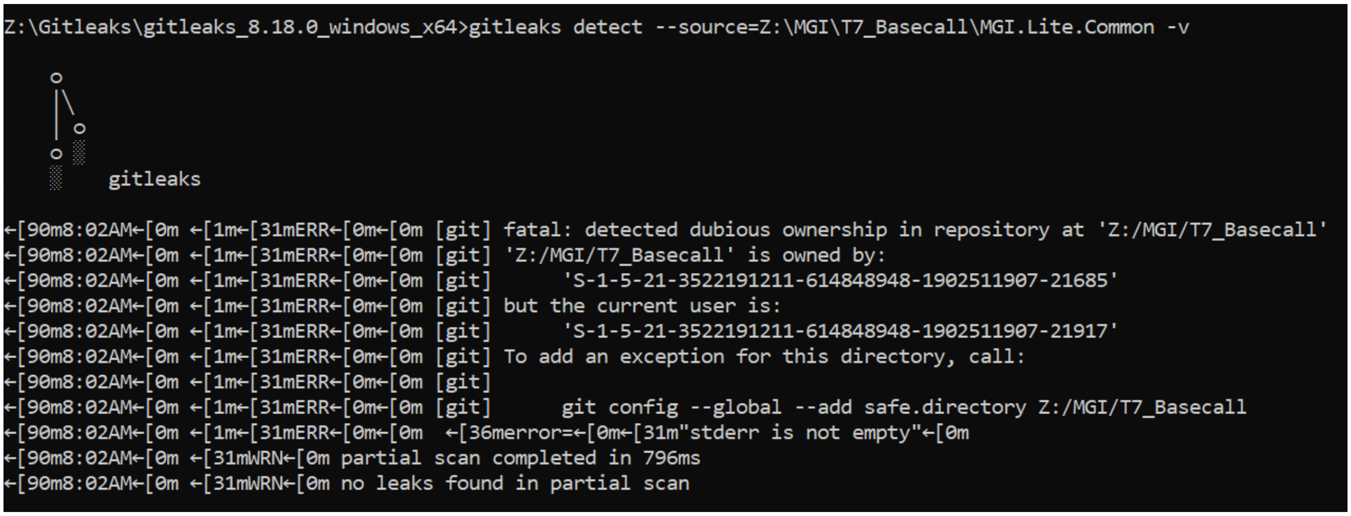
Gitleaks

On October 2, 2023, FTI used Gitleaks to detect whether hardcoded secrets, including tokens, passwords, and API keys, were present in the source code files and parent directories. The command “gitleaks detect” recursively scans the files contained within a specified file path, and the “-v” keyword displays the result in detail.

Initial scans were conducted on the source code using the two paths that the client provided. As seen in Figure 7 and 8 below, there appear to be no leaks found in the scan.

[15] https://github.com/microsoft/etl2pcapng

Figure 7 – Scan of "Z:\MGI\T7_Basecall\MGI.Lite.Common" on 4:12PM Mon Oct 2, 2023

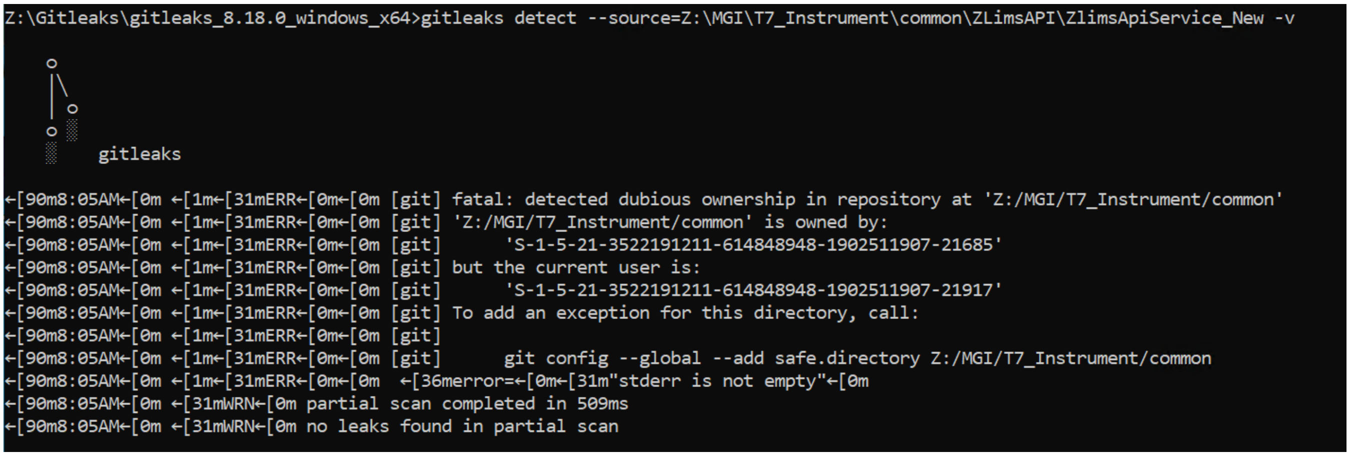


```
Z:\Gitleaks\gitleaks_8.18.0_windows_x64>gitleaks detect --source=Z:\MGI\T7_Basecall\MGI.Lite.Common -v

    ○
    │╲
    │ ○
    ○ ░
    ░   gitleaks

←[90m8:02AM←[0m ←[1m←[31mERR←[0m←[0m [git] fatal: detected dubious ownership in repository at 'Z:/MGI/T7_Basecall'
←[90m8:02AM←[0m ←[1m←[31mERR←[0m←[0m [git] 'Z:/MGI/T7_Basecall' is owned by:
←[90m8:02AM←[0m ←[1m←[31mERR←[0m←[0m [git]      'S-1-5-21-3522191211-614848948-1902511907-21685'
←[90m8:02AM←[0m ←[1m←[31mERR←[0m←[0m [git] but the current user is:
←[90m8:02AM←[0m ←[1m←[31mERR←[0m←[0m [git]      'S-1-5-21-3522191211-614848948-1902511907-21917'
←[90m8:02AM←[0m ←[1m←[31mERR←[0m←[0m [git] To add an exception for this directory, call:
←[90m8:02AM←[0m ←[1m←[31mERR←[0m←[0m [git]
←[90m8:02AM←[0m ←[1m←[31mERR←[0m←[0m [git]      git config --global --add safe.directory Z:/MGI/T7_Basecall
←[90m8:02AM←[0m ←[1m←[31mERR←[0m←[0m  ←[36merror=←[0m←[31m"stderr is not empty"←[0m
←[90m8:02AM←[0m ←[31mWRN←[0m partial scan completed in 796ms
←[90m8:02AM←[0m ←[31mWRN←[0m no leaks found in partial scan
```

Figure 8 – Scan of "Z:\MGI\T7_Instrument\common\ZLimsAPI\ZlimsApiService_New" on 4:20PM Mon Oct 2, 2023



```
Z:\Gitleaks\gitleaks_8.18.0_windows_x64>gitleaks detect --source=Z:\MGI\T7_Instrument\common\ZLimsAPI\ZlimsApiService_New -v

    ○
    │╲
    │ ○
    ○ ░
    ░   gitleaks

←[90m8:05AM←[0m ←[1m←[31mERR←[0m←[0m [git] fatal: detected dubious ownership in repository at 'Z:/MGI/T7_Instrument/common'
←[90m8:05AM←[0m ←[1m←[31mERR←[0m←[0m [git] 'Z:/MGI/T7_Instrument/common' is owned by:
←[90m8:05AM←[0m ←[1m←[31mERR←[0m←[0m [git]      'S-1-5-21-3522191211-614848948-1902511907-21685'
←[90m8:05AM←[0m ←[1m←[31mERR←[0m←[0m [git] but the current user is:
←[90m8:05AM←[0m ←[1m←[31mERR←[0m←[0m [git]      'S-1-5-21-3522191211-614848948-1902511907-21917'
←[90m8:05AM←[0m ←[1m←[31mERR←[0m←[0m [git] To add an exception for this directory, call:
←[90m8:05AM←[0m ←[1m←[31mERR←[0m←[0m [git]
←[90m8:05AM←[0m ←[1m←[31mERR←[0m←[0m [git]      git config --global --add safe.directory Z:/MGI/T7_Instrument/common
←[90m8:05AM←[0m ←[1m←[31mERR←[0m←[0m  ←[36merror=←[0m←[31m"stderr is not empty"←[0m
←[90m8:05AM←[0m ←[31mWRN←[0m partial scan completed in 509ms
←[90m8:05AM←[0m ←[31mWRN←[0m no leaks found in partial scan
```

To ensure thorough testing, FTI used Gitleaks to scan parent directories, namely T7_Instrument, T7_Basecall, and Ztronlite. Results revealed incidences of potential leaks within all three directories, which FTI captured in three output files, and are summarized as follows:

- The command "gitleaks detect --source=Z:\MGI\T7_Instrument --no-git -v" found 92 potential vulnerabilities
- The command "gitleaks detect --source=Z:\MGI\T7_Basecall --no-git -v" found 24 potential vulnerabilities
- The command "gitleaks detect --source=Z:\MGI\Ztronlite--no-git -v" found 114 potential vulnerabilities

Manual review

Using the three output files generated by Gitleaks, FTI analysts created a single, comprehensive Excel file, by cleaning and combining the files and removing duplicate values. Analysts organized the file into two columns, one containing the identified vulnerability in the code, and the other containing the path to the file. FTI analysts inspected the lines of code that were flagged and narrowed down the list, given analysts' immediate identification of false positives. Finally, analysts manually reviewed each of the remaining files to gain a holistic understanding of the context and purpose of the code in which the given vulnerability existed, and additional false positives were eliminated. With the remaining results, FTI analysts conducted regular expression searches to identify sensitive hardcoded information, specifically IP addresses and domain names.

Regular Expressions

FTI analysts conducted regex searches to identify hardcoded IP addresses and domain names within files under the parent directory, and the commands are detailed below. Both searches were conducted on October 3, 2023.

Regex Query for IP addresses in PowerShell at Parent Directory (Z:\MGI):

```
Get-ChildItem -Recurse | Select-String ‘(?<!\S)(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)(?!\S)’
```

Analysts cleaned and analyzed the file containing the results from the regex search on IP addresses, and the results indicated that there were no notable IP addresses found.

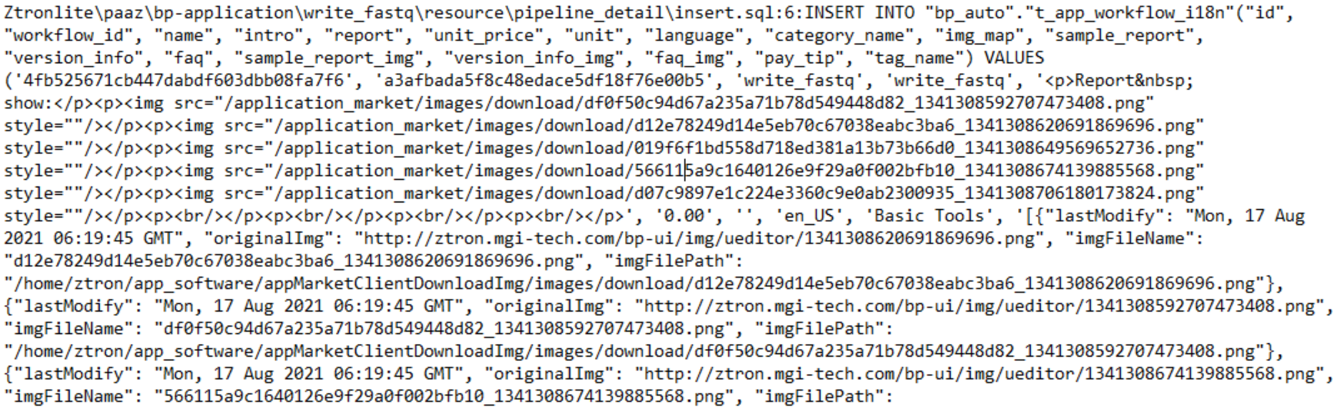
Regex Query for Domain Names in PowerShell at Parent Directory (Z:\MGI):

```
Get-ChildItem -Recurse | Select-String ‘(http[s]?|[s]?ftp[s]?)(:\/\/)([^\s,]+)’ | ForEach-Object { $_.Matches.Value }| Where-Object { $_.Line -notmatch 'schema.microsoft.com|crl.microsoft.com|msdn.microsoft.com|postgresql.org|apache.org' }
```

When searching for domain names, certain domain names were excluded, namely "schema.microsoft.com”, “crl.microsoft.com”, “msdn.microsoft.com”, “postgresql.org”, and “apache.org”, in order to eliminate redundant occurrences of domain names that were not necessary for review as they are out of scope.

FTI analysts identified instances where “ztron.mgi-tech.com” was hardcoded within source code files, as seen in the screenshot of the output in Figure 10. Further inspection of these lines suggests the domain name may be used to download images related to application software, however FTI’s network capture appears to show that the US operation system does not invoke this functionality, as the IP addresses associated with this domain was not observed in network traffic captured by FTI. Based on FTI's network traffic captures, it can be presumed that this functionality was never executed during normal operations, since no IP traffic to/from an IP address related to this domain name was identified as being contacted.

Figure 10 – References of “ztron.mgi-tech.com” to access data



```
Ztronlite\paaz\bp-application\write_fastq\resource\pipeline_detail\insert.sql:6:INSERT INTO "bp_auto"."t_app_workflow_i18n"("id",
"workflow_id", "name", "intro", "report", "unit_price", "unit", "language", "category_name", "img_map", "sample_report",
"version_info", "faq", "sample_report_img", "version_info_img", "faq_img", "pay_tip", "tag_name") VALUES
('4fb525671cb447dabdf603dbb08fa7f6', 'a3afbada5f8c48edace5df18f76e00b5', 'write_fastq', 'write_fastq', '<p>Report&nbsp;
show:</p><p><img src="/application_market/images/download/df0f50c94d67a235a71b78d549448d82_1341308592707473408.png"
style=""/></p><p><img src="/application_market/images/download/d12e78249d14e5eb70c67038eabc3ba6_1341308620691869696.png"
style=""/></p><p><img src="/application_market/images/download/019f6f1bd558d718ed381a13b73b66d0_1341308649569652736.png"
style=""/></p><p><img src="/application_market/images/download/566115a9c1640126e9f29a0f002bfb10_1341308674139885568.png"
style=""/></p><p><img src="/application_market/images/download/d07c9897e1c224e3360c9e0ab2300935_1341308706180173824.png"
style=""/></p><p><br/></p><p><br/></p><p><br/></p><p><br/></p>', '0.00', '', 'en_US', 'Basic Tools', '[{"lastModify": "Mon, 17 Aug
2021 06:19:45 GMT", "originalImg": "http://ztron.mgi-tech.com/bp-ui/img/ueditor/1341308620691869696.png", "imgFileName":
"d12e78249d14e5eb70c67038eabc3ba6_1341308620691869696.png", "imgFilePath":
"/home/ztron/app_software/appMarketClientDownloadImg/images/download/d12e78249d14e5eb70c67038eabc3ba6_1341308620691869696.png"},
{"lastModify": "Mon, 17 Aug 2021 06:19:45 GMT", "originalImg": "http://ztron.mgi-tech.com/bp-ui/img/ueditor/1341308592707473408.png",
"imgFileName": "df0f50c94d67a235a71b78d549448d82_1341308592707473408.png", "imgFilePath":
"/home/ztron/app_software/appMarketClientDownloadImg/images/download/df0f50c94d67a235a71b78d549448d82_1341308592707473408.png"},
{"lastModify": "Mon, 17 Aug 2021 06:19:45 GMT", "originalImg": "http://ztron.mgi-tech.com/bp-ui/img/ueditor/1341308674139885568.png",
"imgFileName": "566115a9c1640126e9f29a0f002bfb10_1341308674139885568.png", "imgFilePath":
```

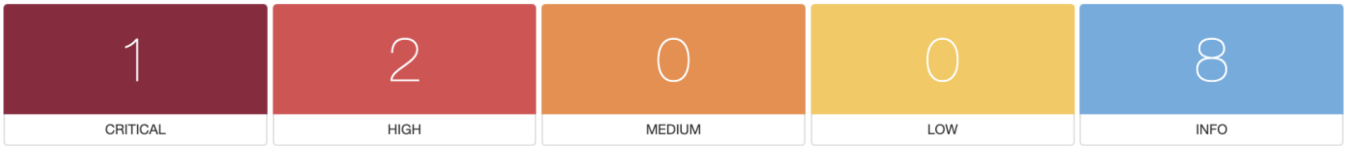
3.2.3 Vulnerability Scans

All three scanned hosts contained several “Informational” vulnerabilities, which do not present an immediate danger to any systems or services. These findings are strictly informational and in theory could provide useful information to a would-be attacker. Since these findings are numerous and not deemed severe, FTI has not included them in this overview, however these findings will be provided upon request.

T7 Windows Host (SBC)

Start time: Thu Aug 31 11:16:41 2023 UTC

IP Address at Time of Scan: 192.168.100.12



1	2	0	0	8
CRITICAL	HIGH	MEDIUM	LOW	INFO

Critical Vulnerabilities:

- Outdated CodeMeter Version Contain Multiple Vulnerabilities.

According to its self-reported version, the CodeMeter WebAdmin server installed on the remote host is prior to 7.10a. It is, therefore, affected by multiple vulnerabilities.

- https://nvd.nist.gov/vuln/detail/CVE-2020-14509
- https://nvd.nist.gov/vuln/detail/CVE-2020-14517
- https://nvd.nist.gov/vuln/detail/CVE-2020-14519

High Severity Vulnerabilities

- Outdated CodeMeter Version Allows for License Forging

According to its self-reported version, the CodeMeter WebAdmin server installed on the remote host is prior to 6.90. It is affected by an issue in the license-file signature checking mechanism, which allows attackers to build arbitrary license files, including forging a valid license file as if it were a valid license file of an existing vendor. Only CmActLicense Update Files with CmActLicense Firm Codes are affected.

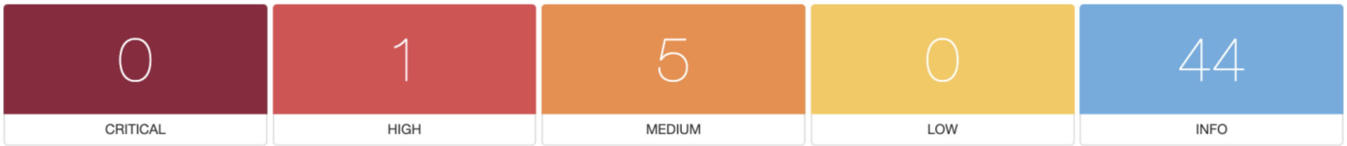
- https://nvd.nist.gov/vuln/detail/CVE-2020-14515

Depending on system setup, specifically whether this OS is connected to the internet or other devices, these CodeMeter vulnerabilities could allow for remote communication, potentially providing an attacker an avenue to full access and control over a compromised device.

Mechanical Controller Windows Host (BCS)

Start Time: Thu Aug 31 10:45:49 2023 UTC

IP Address at Time of Scan: 192.168.0.5



CRITICAL	HIGH	MEDIUM	LOW	INFO
0	1	5	0	44

High Severity Vulnerabilities:

- Medium Strength SSL Cipher Suite Supported

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

- https://nvd.nist.gov/vuln/detail/CVE-2016-2183

Medium Severity Vulnerabilities:

- SMB Signing not Required

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

— https://learn.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/cc731957(v=ws.11)?redirectedfrom=MSDN

- SSL Certificate Cannot be Trusted

The server's X.509 certificate can become untrusted due to three possible issues in the chain of trust: firstly, when the certificate chain isn't rooted in a recognized public certificate authority, which can happen with self-signed certificates or missing intermediate certificates; secondly, if the chain contains certificates that are invalid at the time of scanning, either before the 'notBefore' date or after the 'notAfter' date; and thirdly, when the chain contains a signature mismatch or an unverifiable signature, often caused by unsupported signing algorithms. For public hosts in production, any break in this chain hinders user authentication and increases vulnerability to man-in-the-middle attacks.

- SSL Self Signed Certificate

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

- Outdated TLS Version in Use

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

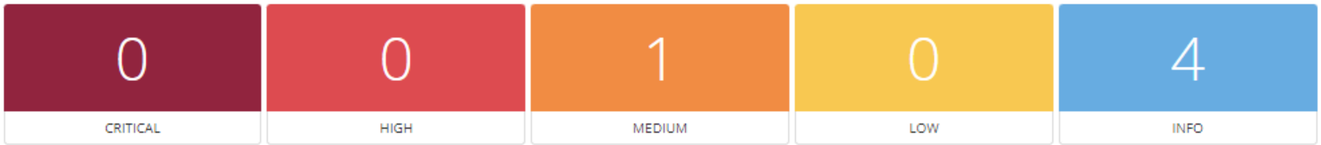
— https://cwe.mitre.org/data/definitions/327

The above vulnerabilities primarily relate to SSL vulnerabilities, which poses a less likely threat based on anticipated use and setup of BCS, as learned from August 30, 2023 conversations.

ZTRON CentOS Linux Host

Start Time: Sun Oct 1 00:21:03 2023 UTC

IP Address at Time of Scan: 192.168.1.3



0	0	1	0	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Medium Severity Vulnerability:

- mDNS Detection (Remote Network)

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

3.2.4 Hardware Schematics Review

FTI identified no inconsistencies in the hardware schematic design, design rules, schematic conventions, and documentation related to the ZTRON. FTI assesses that CG's schematic diagrams are of a high-quality design and engineering work product. Observations are included in Appendix E.

4. CONCLUSION

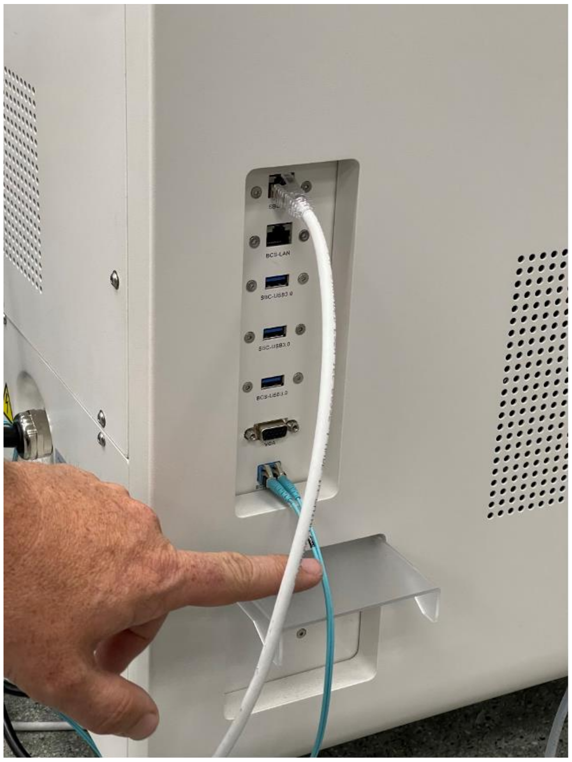
FTI's approach revealed that the ZTRON and T7 functionality contained within CG's US version 1) did not result in outbound, external IP communications during genomic sequencing aside from that required for Linux system functionality; 2) did not contain immediately concerning source code or network vulnerabilities; and 3) otherwise appeared consistent with expected hardware design.

5. APPENDIX A: External IP Addresses Found

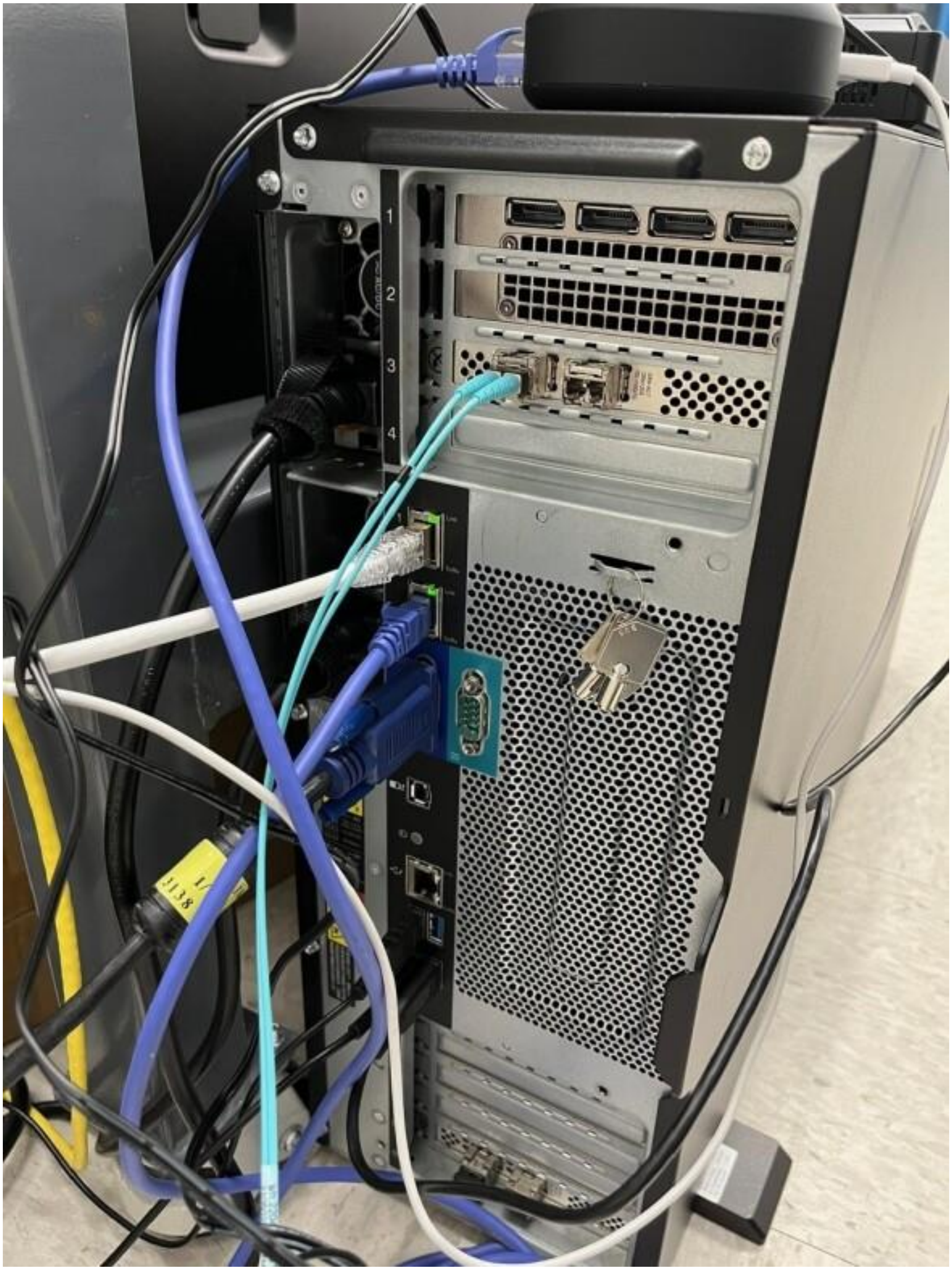
IP	Resolved Domain	Country of Origin
129.21.171.72	zuul.rc.rit.edu	United States
130.111.32.173	lv-o-mirrors2.its.maine.edu	United States
142.147.88.7	142.147.88.7.static.xtom.com	United States
144.26.0.246	mirrors.wcupa.edu	United States
184.105.240.111	mirror.keystealth.org	United States
198.129.224.35	linux.mirrors.es.net	United States
209.58.135.187	mirror.sfo12.us.leaseweb.net	United States
216.31.0.2	team-cymru.org	United States
66.244.16.51	unallocated-16-244-66.shastacoe.net	United States
69.167.187.144	mirrors.liquidweb.com	United States
204.93.207.12	tick.chi1.ntfo.org	United States
209.51.161.238	clock.nyc.he.net	United States
66.228.59.187	fairy0.mattnordhoffdns.net	United States
165.140.142.118	ns.bgp.co	United States
74.207.242.234	beta.kenyonralph.com	United States
216.229.0.50	nu.binary.net	United States
209.51.161.238	clock.nyc.he.net	United States
44.190.5.123	0.suse.pool.ntp.org	United States
151.204.223.236	pool-151-204-223-236.nwrknj.fios.verizon.net	United States
192.112.36.4	G.ROOT-SERVERS.NET	United States
192.5.5.241	f.root-servers.net	United States
154.16.113.160	or-mirror.iwebfusion.net	United States
154.16.113.160	or-mirror.iwebfusion.net	United States
23.27.126.50	opencolo.mm.fcix.net	United States
77.247.126.176	la.mirrors.clouvider.net	United States
157.131.224.201	mirrors.sr.sonic.net	United States
23.152.160.16	mirror.fcix.net	United States
169.229.200.70	mirrors.ocf.berkeley.edu	United States
192.69.77.209	mnvoip.mm.fcix.net	United States
192.154.203.33	nc-mirror.iwebfusion.net	United States
207.244.94.80	mirror.wdc2.us.leaseweb.net	United States
147.160.170.17	southfront.mm.fcix.net	United States
206.82.17.213	mirrors.iu13.net	United States
128.173.237.17	mirror.cs.vt.edu	United States
209.222.200.200	FCIX-LINUX-MIRROR.maineren.net	United States
84.247.2.31	as117.vacares.com	United States

134.195.207.11	mm.fcix.ohioix.net	United States
204.157.3.70	mirror.cogentco.com	United States
132.198.255.58	uvermont.mm.fcix.net	United States
131.225.105.75	linux-mirrors.fnal.gov	United States
163.237.219.7	ftpmirror.your.org.219.237.163.in-addr.arpa	United States
192.170.231.249	mirror.grid.uchicago.edu	United States
23.189.48.83	paducahix.mm.fcix.net	United States
23.147.64.7	forksystems.mm.fcix.net	United States
161.129.154.250	mirror.dal.nexril.net	United States
50.47.0.53	ziply.mm.fcix.net	United States

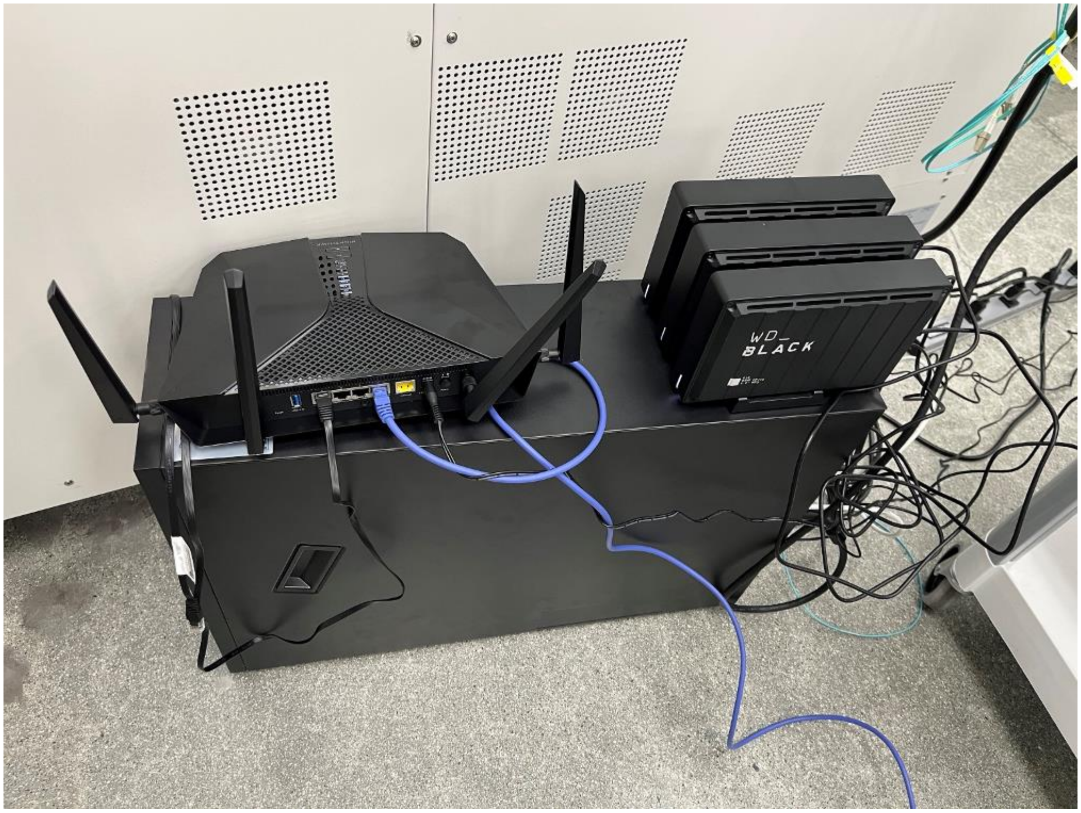
6. APPENDIX B: T7 Exterior/Interior View and I/O Ports

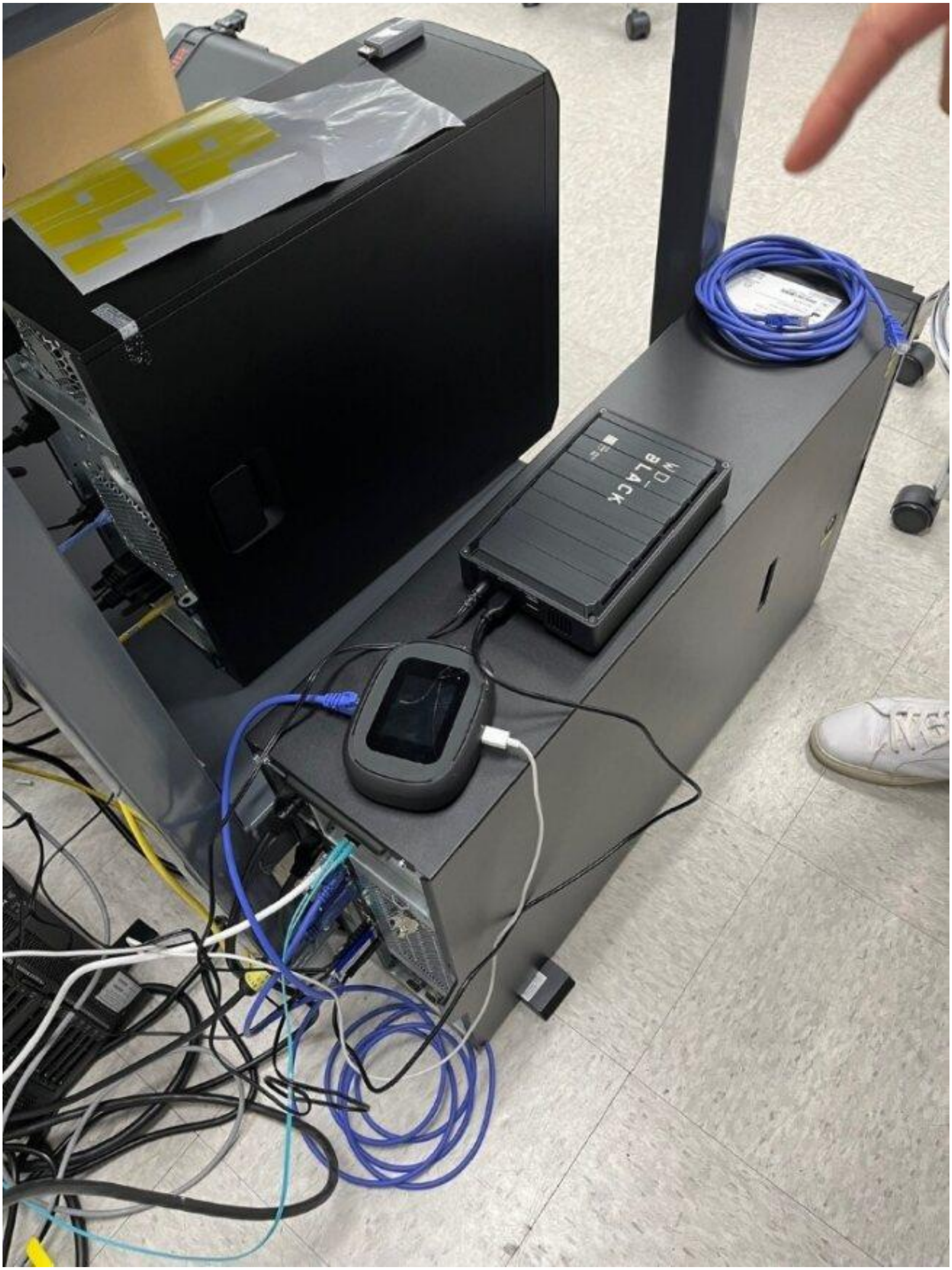


7. APPENDIX C: ZTRON Back View

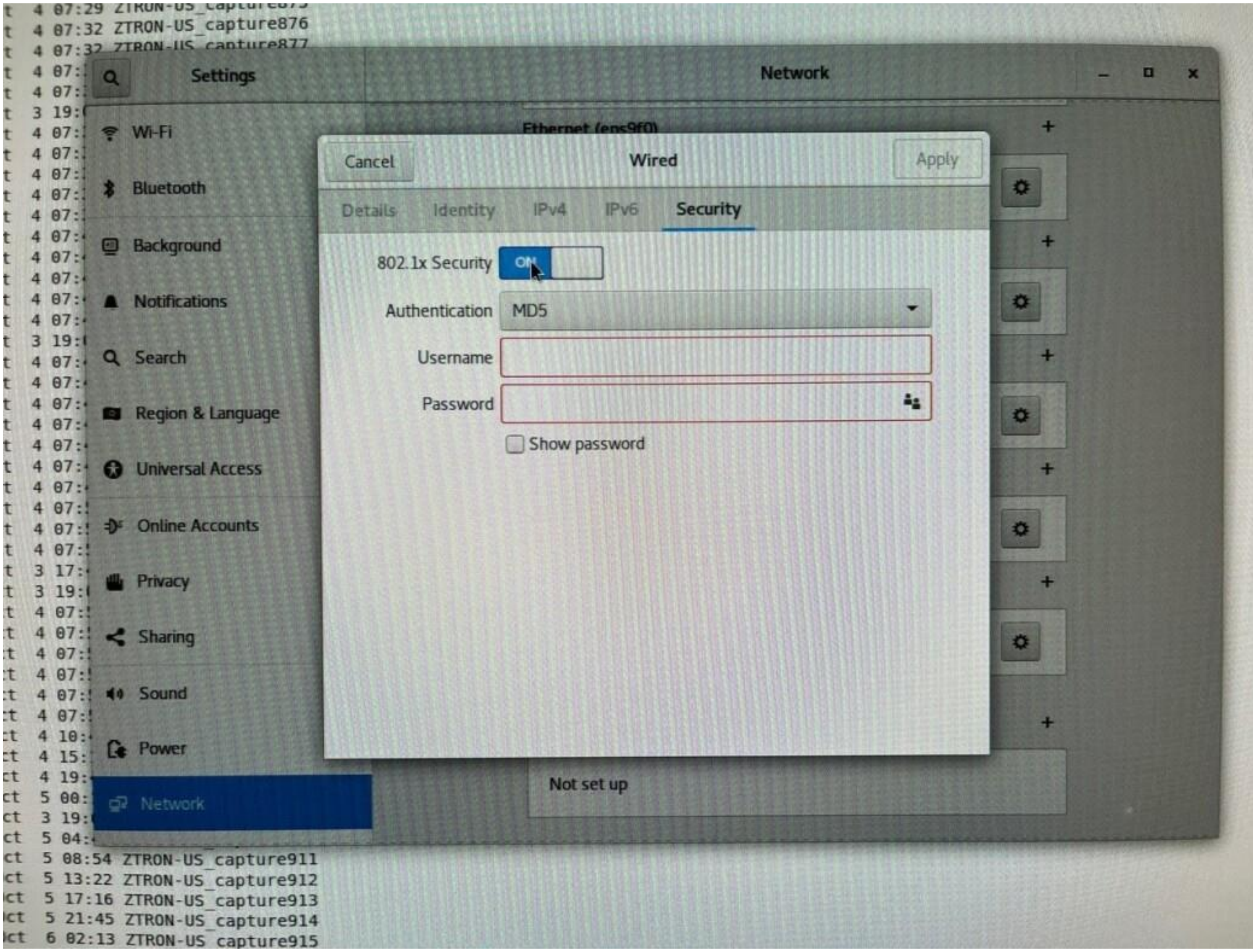


8. APPENDIX D: ZTRON Configuration for Vulnerability Scanning and Network Capture





WD_BLACK



```
t  4 07:29 ZTRON-US_capture875
t  4 07:32 ZTRON-US_capture876
t  4 07:32 ZTRON-US_capture877
t  4 07:
t  4 07:
t  3 19:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  3 19:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  3 17:
t  3 19:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 07:
t  4 10:
t  4 15:
ct  4 19:
ct  5 00:
ct  3 19:
ct  5 04:
ct  5 08:54 ZTRON-US_capture911
ct  5 13:22 ZTRON-US_capture912
ct  5 17:16 ZTRON-US_capture913
ct  5 21:45 ZTRON-US_capture914
ct  6 02:13 ZTRON-US_capture915
```

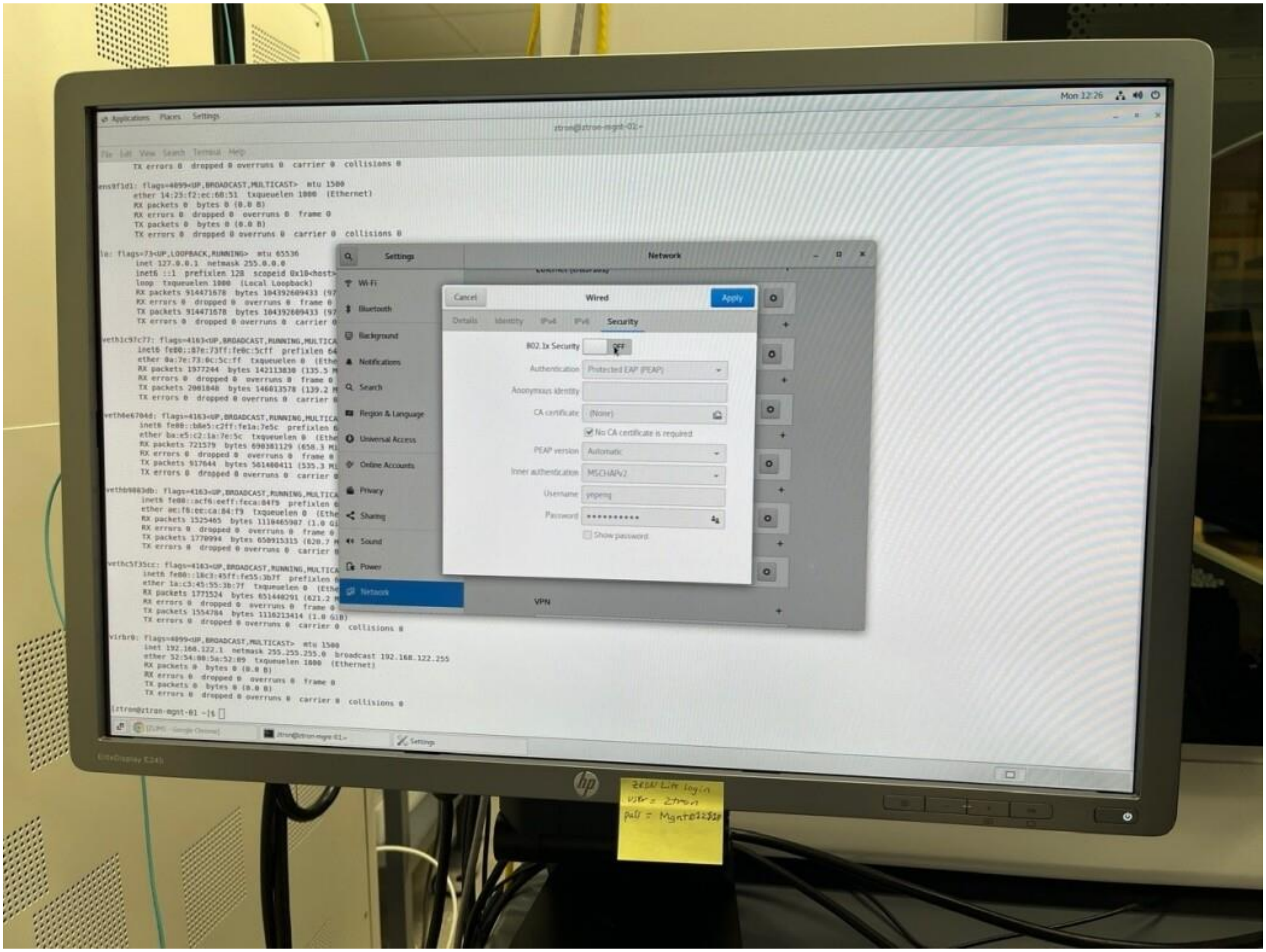
802.1x Security: ON

Authentication: MD5

Username:

Password:

□ Show password



Applications Places Settings
Mon 12:26
ztron@ztron-mgnt-01:~
File Edit View Search Terminal Help

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens9f1d1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 14:23:f2:ec:60:51  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 914471678  bytes 104392609433 (97
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 914471678  bytes 104392609433 (97
        TX errors 0  dropped 0 overruns 0  carrier 0

veth1c97c77: flags=4163<UP,BROADCAST,RUNNING,MULTICA
        inet6 fe80::87e:73ff:fe0c:5cff  prefixlen 64
        ether 0a:7e:73:0c:5c:ff  txqueuelen 0  (Ethe
        RX packets 1977244  bytes 142113830 (135.5 M
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2001840  bytes 146013578 (139.2 M
        TX errors 0  dropped 0 overruns 0  carrier 0

veth6e6704d: flags=4163<UP,BROADCAST,RUNNING,MULTICA
        inet6 fe80::b8e5:c2ff:fe1a:7e5c  prefixlen 6
        ether ba:e5:c2:1a:7e:5c  txqueuelen 0  (Ethe
        RX packets 721579  bytes 690381129 (658.3 Mi
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 917644  bytes 561480411 (535.3 Mi
        TX errors 0  dropped 0 overruns 0  carrier 0

vethb9883db: flags=4163<UP,BROADCAST,RUNNING,MULTICA
        inet6 fe80::acf6:eeff:feca:84f9  prefixlen 6
        ether ae:f6:ee:ca:84:f9  txqueuelen 0  (Ethe
        RX packets 1525465  bytes 1110465987 (1.0 Gi
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1770994  bytes 650915315 (620.7 M
        TX errors 0  dropped 0 overruns 0  carrier 0

vethc5f35cc: flags=4163<UP,BROADCAST,RUNNING,MULTICA
        inet6 fe80::18c3:45ff:fe55:3b7f  prefixlen 6
        ether 1a:c3:45:55:3b:7f  txqueuelen 0  (Ethe
        RX packets 1771524  bytes 651440291 (621.2 M
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1554784  bytes 1110213414 (1.0 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:5a:52:09  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[ztron@ztron-mgnt-01 ~]$ 
```

Network

Wired

802.1x Security: OFF

Authentication: Protected EAP (PEAP)

Anonymous identity:

CA certificate: (None)

☑ No CA certificate is required

PEAP version: Automatic

Inner authentication: MSCHAPv2

Username: yepeng

Password: ••••••••••

☐ Show password

ZRON Lite login
user = ztron
pass = Mgnt@12$$#

9. APPENDIX E: Hardware Schematics Review

Per review of ZTRON schematics documents titled “ST650V2.pdf” and “ZtronLite motherboard.png” provided by CG, FTI made the following observations:

- There are two ethernet ports that can be used for connection
- There is a USB port that is used for connection to mobile devices
  - This connection is supported through the XCC and has had a vulnerability in the past CVE-2022-34888
  - The schematic and documentation are all in align with each other, along with the documentation and consistent with Lenovo’s published material
  - This allows for remote management (while connected and through the XCC app on mobile) and is provided through industry standard interfaces (IMPI 2.0, SNMP3, CIM-XML, REST support, Redfish, Web NLS support)
- Utilizing the NVMes requires a different configuration than when utilizing the PCIe slots in the ST650 V2. All are configured correctly
  - Slot 8 is optional and can only be used with connection to the NVMes

TODD RENNER
Senior Managing Director
Atlanta, GA
+1 404 460 6200
Todd.renner@fticonsulting.com

MATT CHEVRAUX
Managing Director
Washington, DC
+1 202 394 5480
Matt.chevraux@fticonsulting.com

ENRIQUE ALVAREZ
Managing Director
San Francisco, CA
+1 240 853 3172
Enrique.alvarez@fticonsulting.com

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. Connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn. **www.fticonsulting.com**

EXPERTS WITH IMPACT™