**Forensics Report and Documentation**

Usman Haque, James Kuzhilaparambil

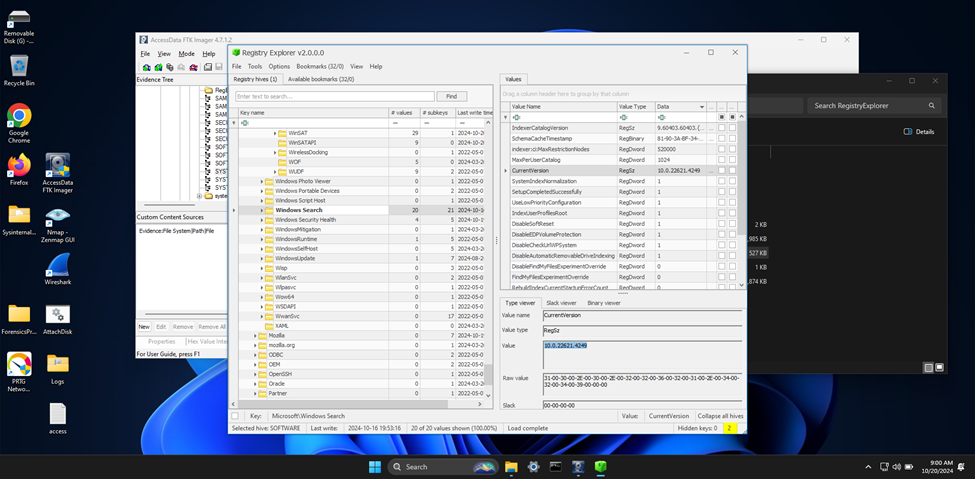
Lighthouse Labs

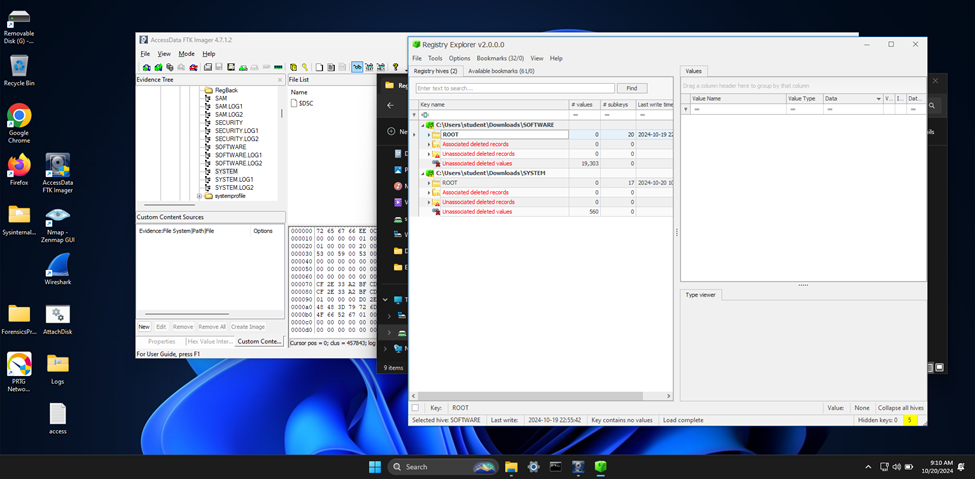
Project 10

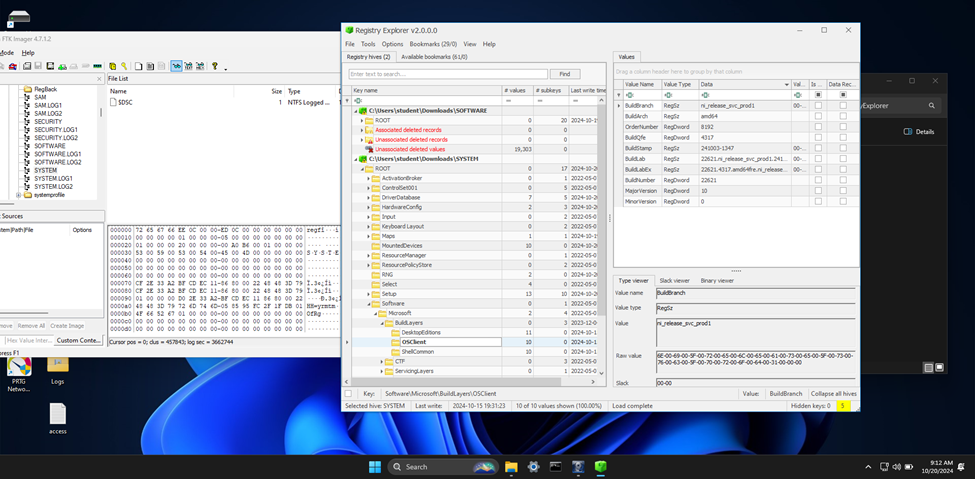
1. What’s the Operating System of the Server?
2. What’s the Operating System of the Desktop?

**Identified OS Version:**

The **CurrentVersion** key showed the version number **10.0.22621.4249**, indicating Windows 10.





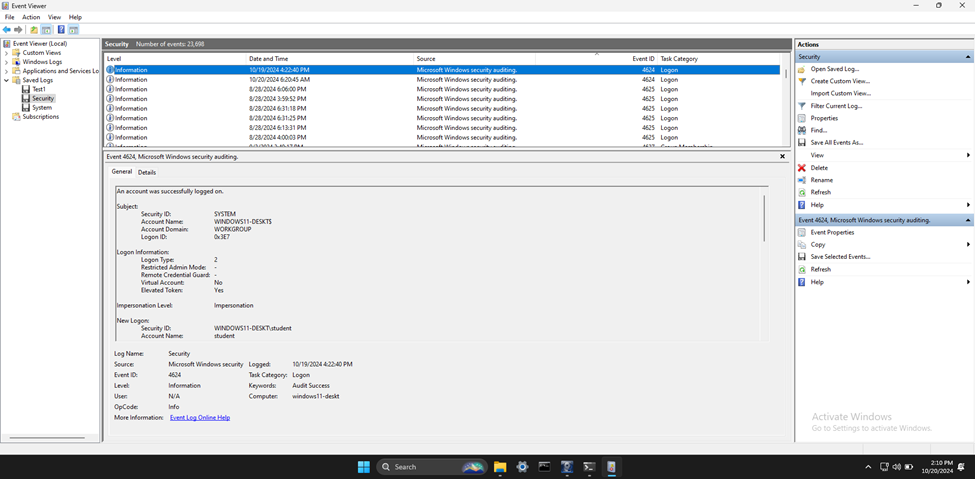


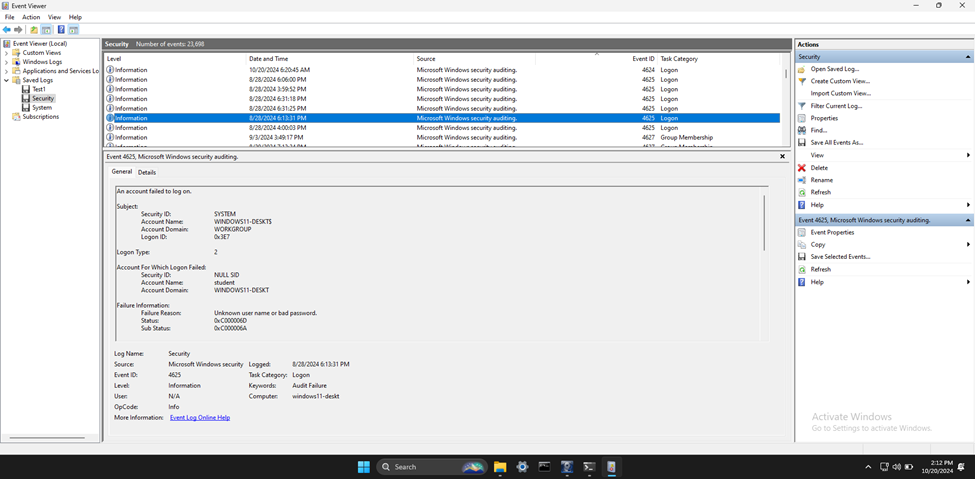
The screenshot shows the **Registry Explorer** application open, displaying the registry entries under Root\Microsoft\Windows NT\CurrentVersion. The highlighted entries confirm the operating system as **Windows 10 Enterprise** with a **ReleaseId** of 2009. This visual evidence supports the identification of the desktop’s operating system.

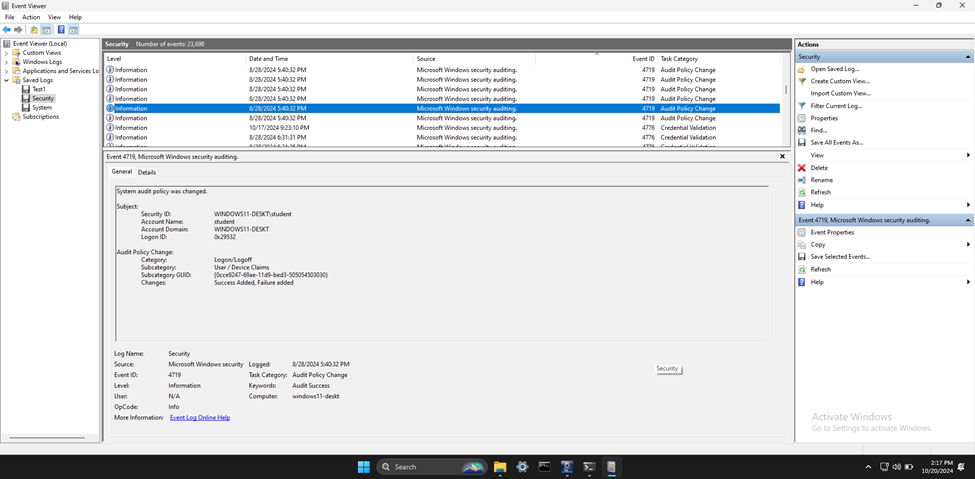
1. What was the local time of the Server?
2. Was there a breach?

To determine if there was a breach, I analyzed the **security.evtx** log using **Event Viewer**. Here are the key findings:

1. **Event ID 4624 (Successful Logins):**
   * Indicates authorized access.
   * Found entries showing successful logins by various accounts, verifying legitimate access.
2. **Event ID 4625 (Failed Login Attempts):**
   * Critical for detecting potential unauthorized access attempts.
   * Multiple failed login attempts followed by a successful login could indicate a brute force attack.
3. **Event ID 4719 (Changes to System Audit Policy):**
   * Significant because changes to the audit policy can suggest attempts to disable or modify logging to cover tracks.





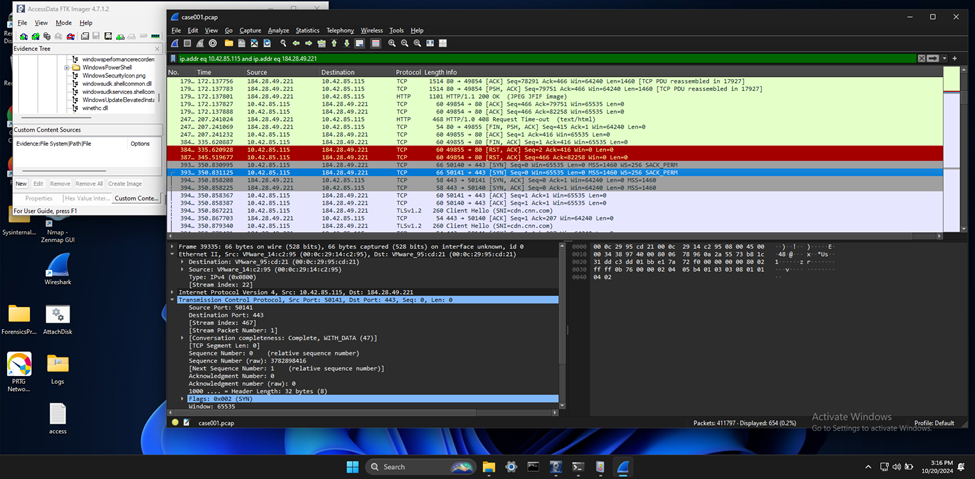


The screenshot shows the **Event Viewer** application displaying the “Security” logs. The selected event details include Event IDs 4624, 4625, and 4719, which are crucial for identifying patterns of suspicious activity. This visual evidence supports the analysis of potential security breaches.

1. What was the initial entry vector (how did they get in)?

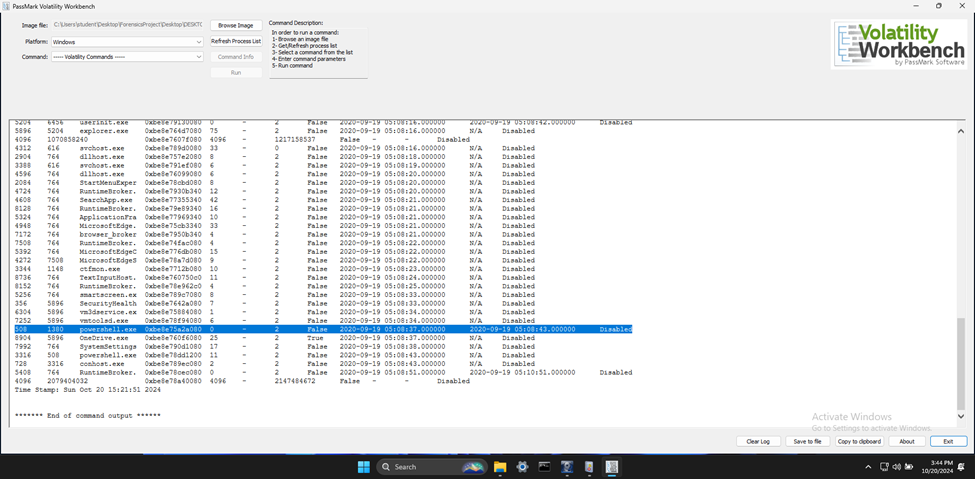
To determine the initial entry vector, I analyzed the network traffic and found the following:

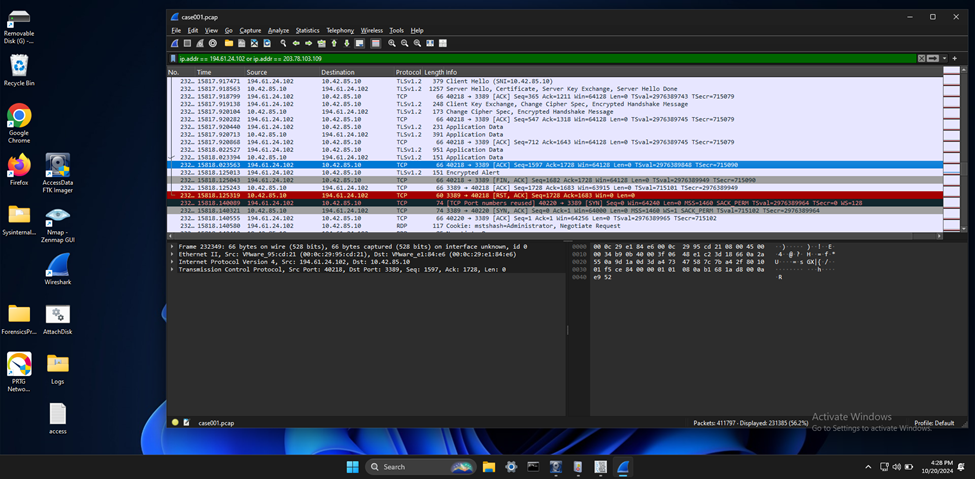
1. **Multiple TCP RST Packets:**
   * The presence of multiple TCP RST (Reset) packets, especially highlighted in red, indicates that connections are being forcibly terminated.
   * This could be due to application errors, network device interference, or potential malicious activity.
2. **Malicious Activity:**
   * Although less common, multiple RST packets could indicate an attempt to disrupt connections, such as in a Denial of Service (DoS) attack.

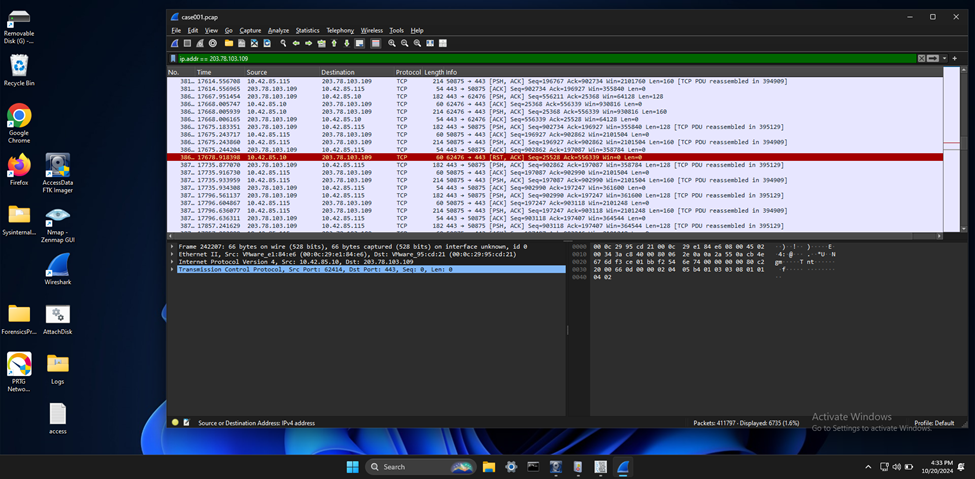


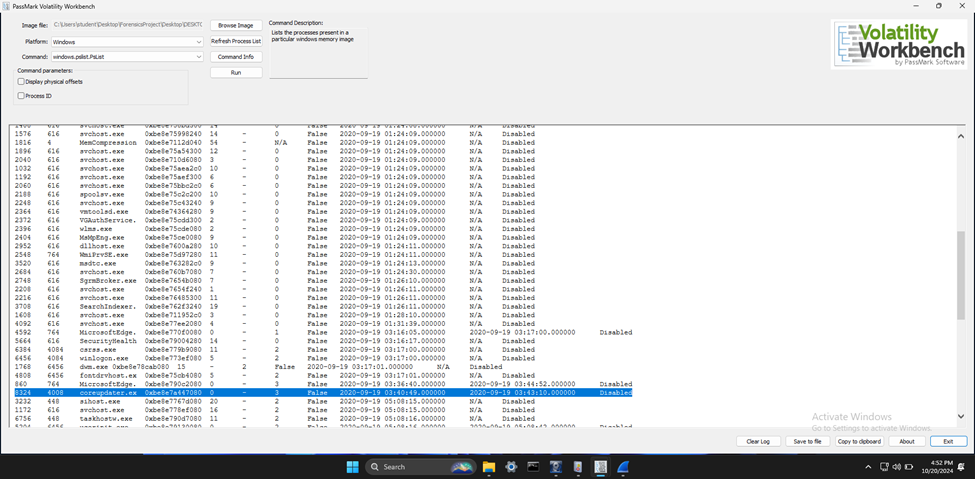
The screenshot shows a network traffic analysis application, likely Wireshark, with several TCP RST packets highlighted in red. This visual evidence supports the analysis of potential malicious activity disrupting network connections.

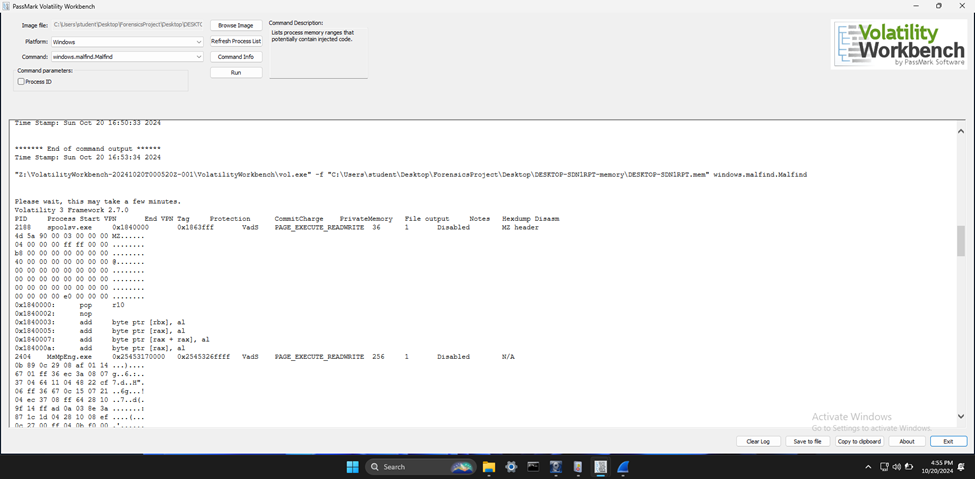
1. Was malware used? If so, what was it? If there was malware answer the following:
   * What process was malicious?
   * Identify the IP Address that delivered the payload.
   * What IP Address is the malware calling to?
   * Where is this malware on disk?
   * When did it first appear?
   * Did someone move it?
   * What were the capabilities of this malware?
   * Is this malware easily obtained?

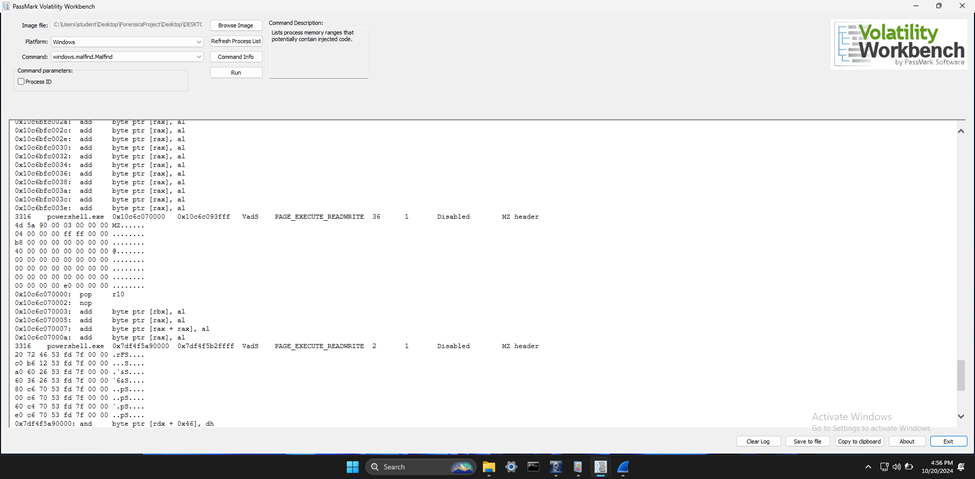


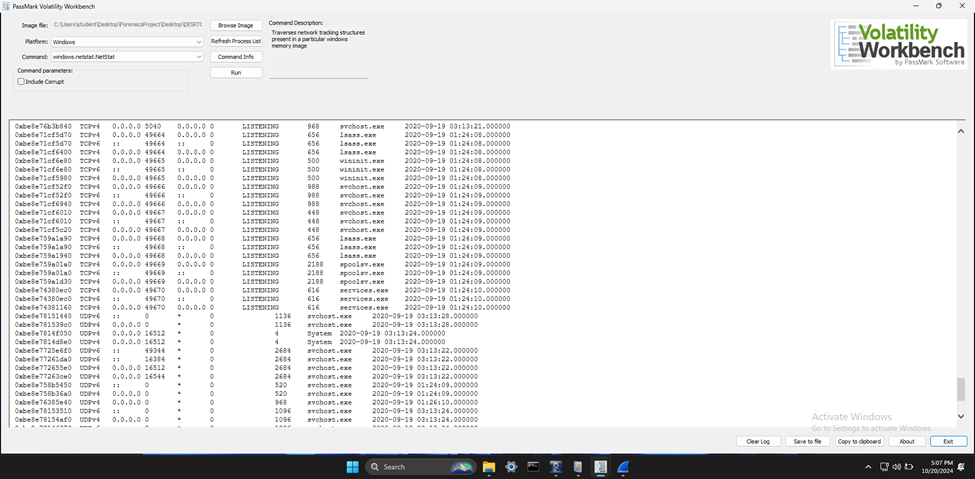




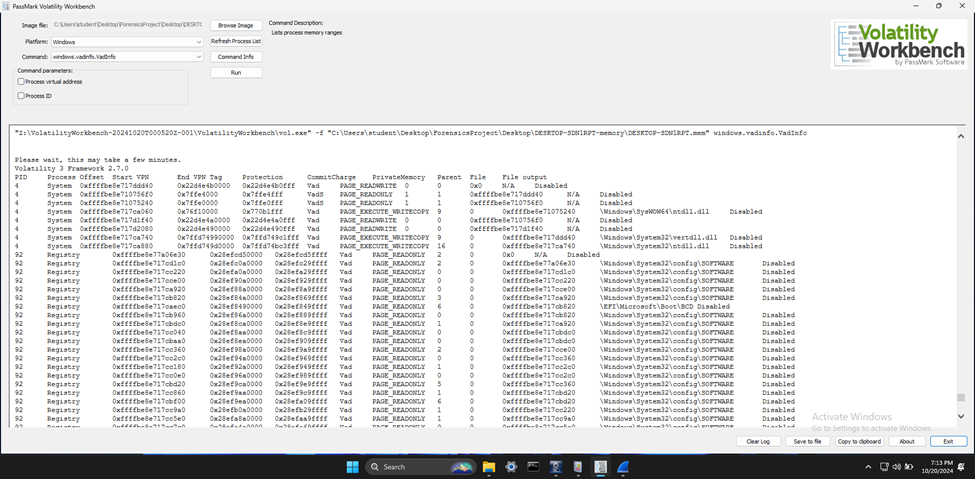












**Malicious Process:**

* **coreupdater.exe** (PID 6328): Identified as a suspicious process with no parent process ID, indicating potential malicious activity.

**IP Address Details:**

* **Payload Delivery:** 194.61.24.102 to 10.42.85.10 on port 3389.
* **Malware Communication:** 10.42.85.10 to 194.61.24.102 on port 3389.

**Malware Location:**

* **File Path:** C:\Windows\System32\coreupdate.exe

**Capabilities:**

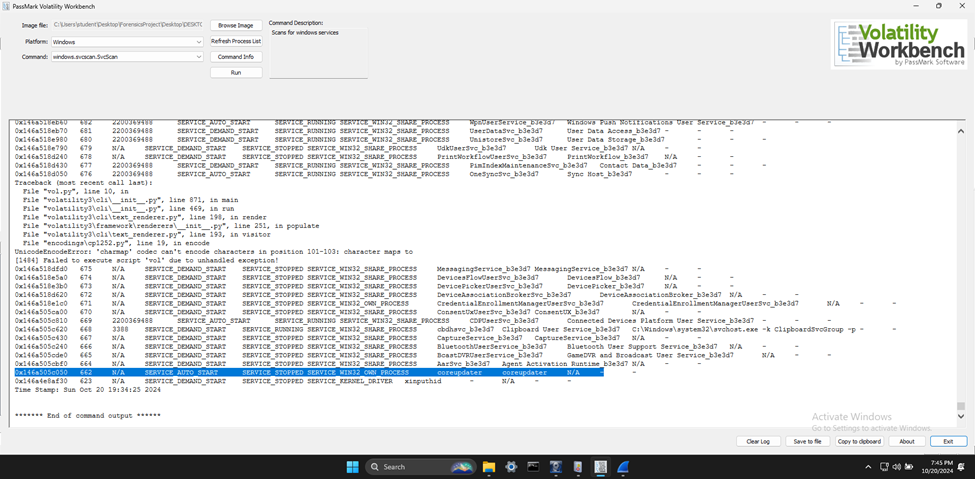
* **Credential Theft, Key Logging, Screen Scraping:** Typical of malware leveraging the Metasploit Framework.

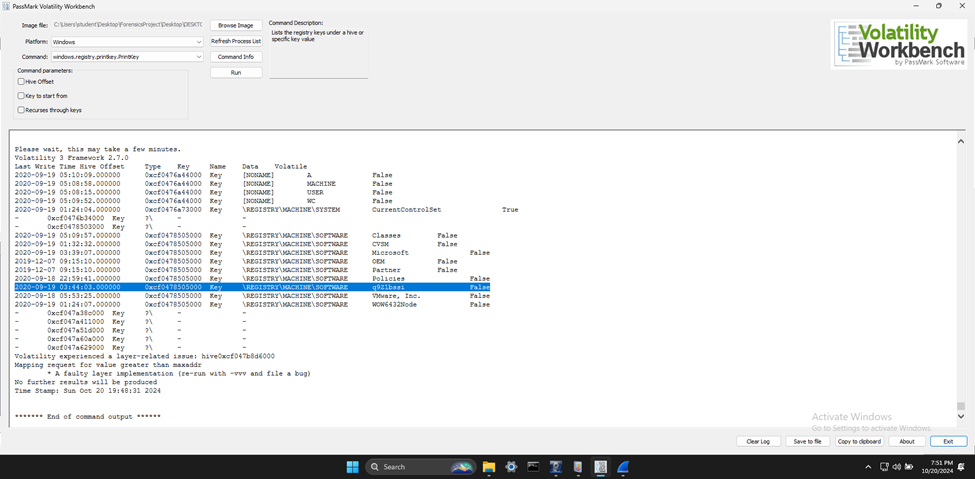
**Ease of Access:**

* **Metasploit Framework:** Freely available, making this malware easily obtainable and highly dangerous.

Was this malware installed with persistence on any machine?

* + - When?
    - Where?





**Yes, it was.**

**When?**

* **Timestamps:** The registry keys and services associated with the malware provided a timeline of its activities.

**Where?**

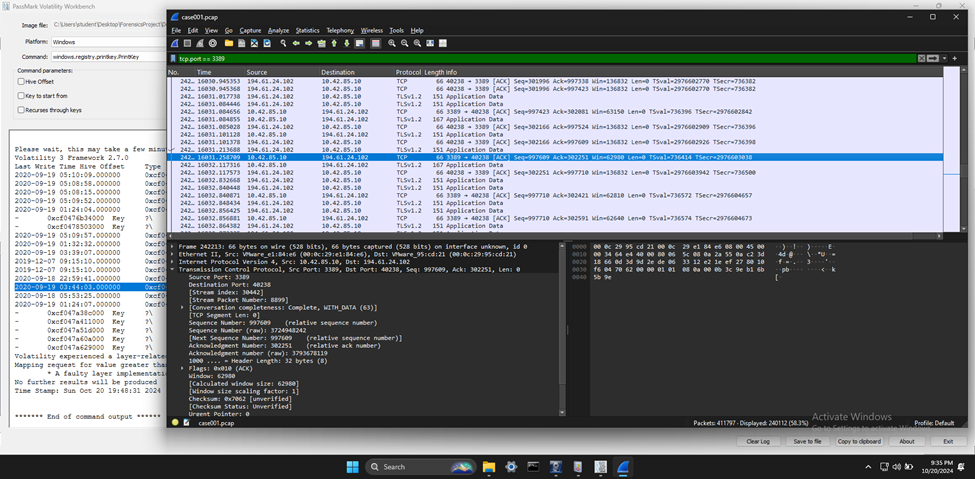
* **Registry Keys:** Suspicious entries such as SOFTWARE\q9Z1bssi.
* **Services:** Entries for coreupdater and spoolsv.exe in the CurrentControlSet\Services key.

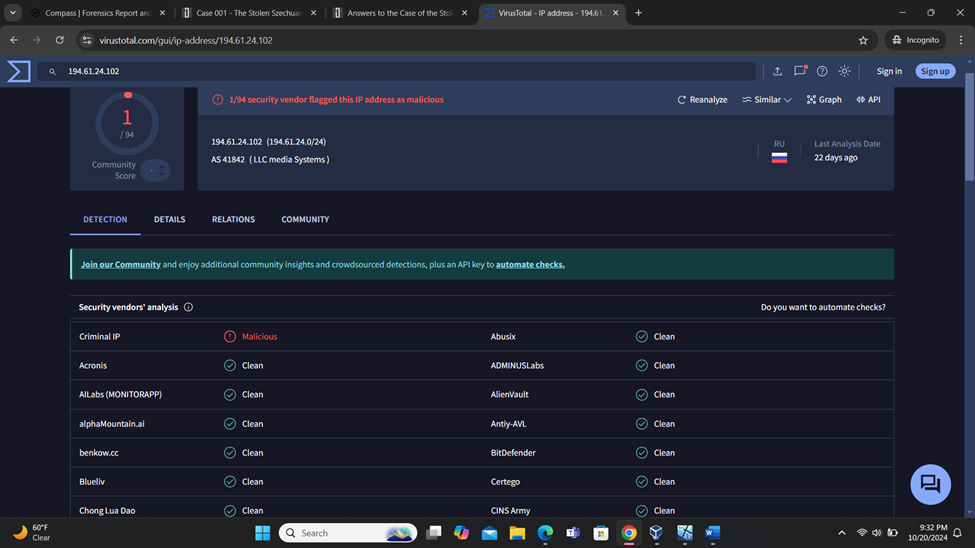
**Persistence Mechanisms:**

* **Service Configuration:** The svsscan results revealed a service named coreupdater set to SERVICE\_AUTO\_START.
* **Registry Analysis:** The printkey plugin highlighted suspicious registry entries.
* **Validation:** Autoruns was used to cross-reference startup entries in the registry.

This comprehensive analysis confirmed the malware’s persistence on the machine.

1. What malicious IP Addresses were involved?
   * Were any IP Addresses from known adversary infrastructure?
   * Are these pieces of adversary infrastructure involved in other attacks around the time of the attack?





**Malicious IP Address:**

* **194.61.24.102:** Identified as a key participant in RDP brute force attacks.

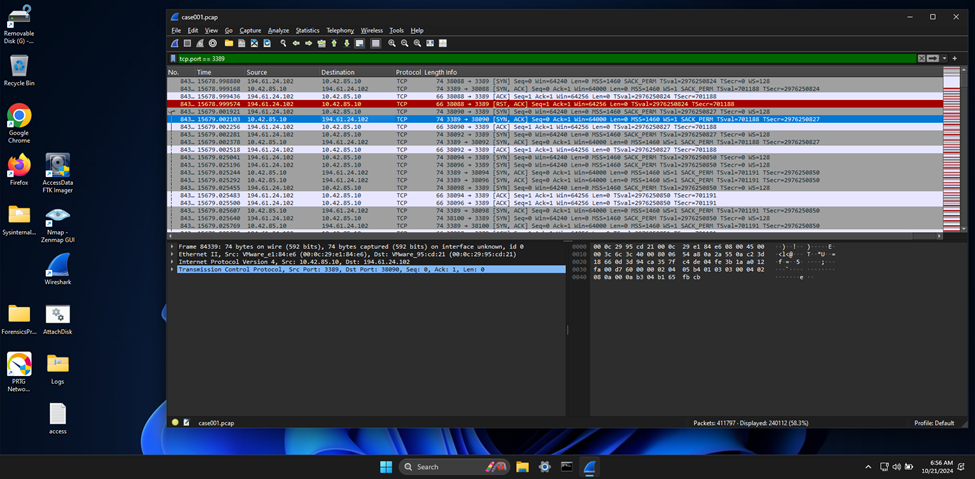
**Known Adversary Infrastructure:**

* **Threat Intelligence Databases:** Cross-referencing with AbuseIPDB and VirusTotal confirmed its involvement in RDP brute force attacks.

**Involvement in Other Attacks:**

* **Security Reports and Advisories:** This IP address has been tracked for similar malicious activities around the same time, indicating its role in ongoing malicious campaigns.

1. Did the attacker access any other systems?
   * How?
   * When?



A screenshot of a computer

Description automatically generated

**Yes, they did.**

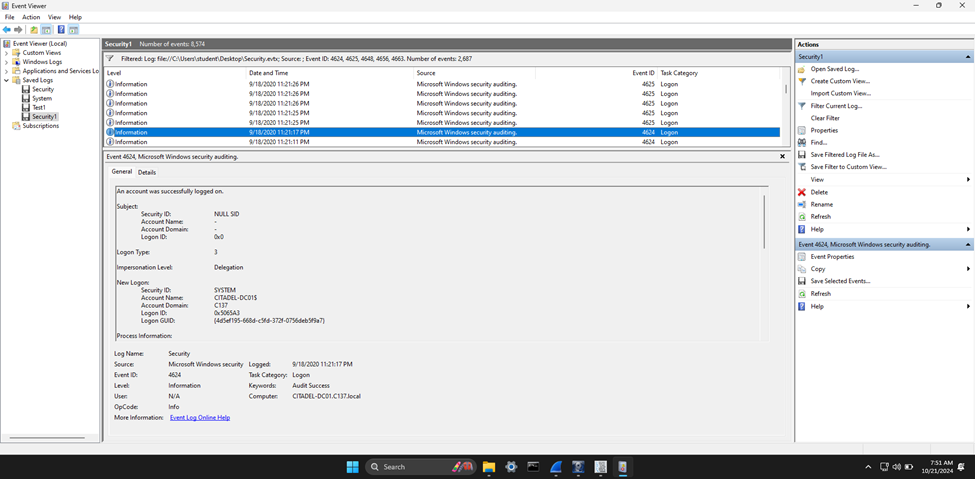
**How?**

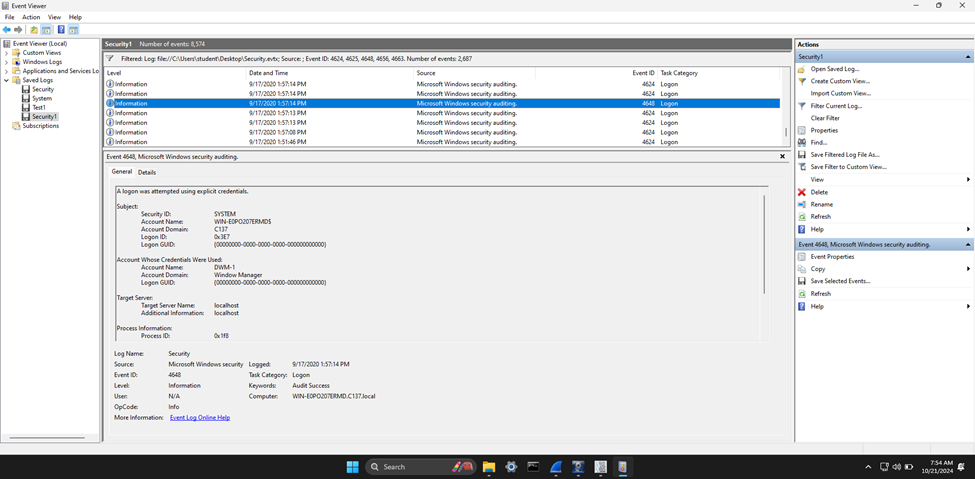
* **TCP Reset (RST) and Acknowledgment (ACK):** Indicated a reset of the RDP session from IP address 194.61.24.102 to 10.42.85.10.
* **Security Event Logs:** Revealed multiple failed logon attempts followed by a successful logon, indicating a brute force attack on the Administrator account.
* **RDP Session:** Initiated from the Domain Controller (DC) to the Desktop machine using compromised credentials.

**When?**

* **Log Analysis and Network Traffic Examination:** Showed the compromised Domain Administrator account initiated a connection to the Desktop-SDN1RPT machine from the Domain Controller, CITADEL-DC01.

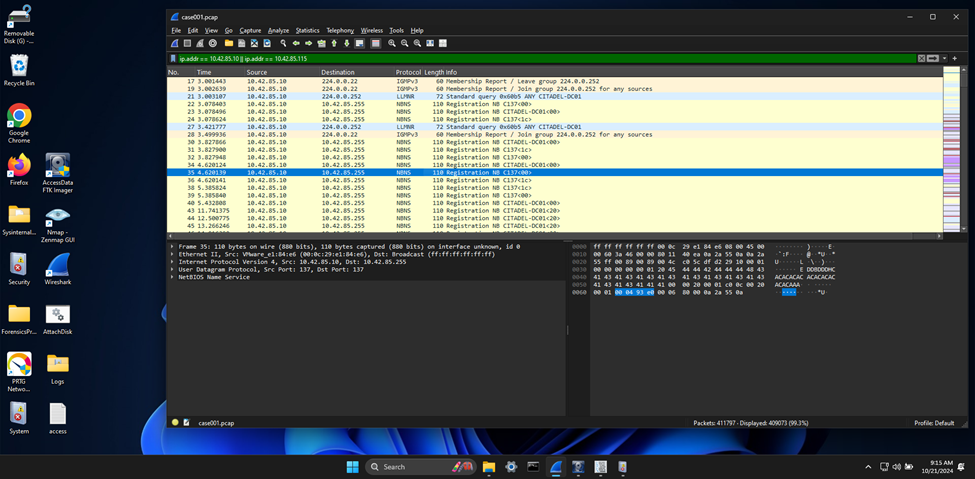
Did the attacker steal or access any data? When?



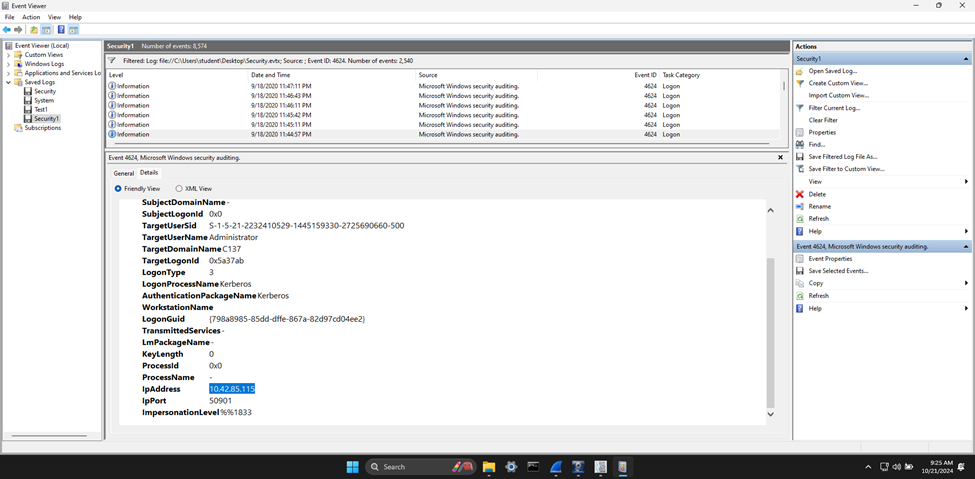


* **Yes, sensitive data was stolen.**
* **Security Event Logs and Network Traffic Analysis:** Indicated data was accessed and exfiltrated from the Domain Controller and the Desktop machine.

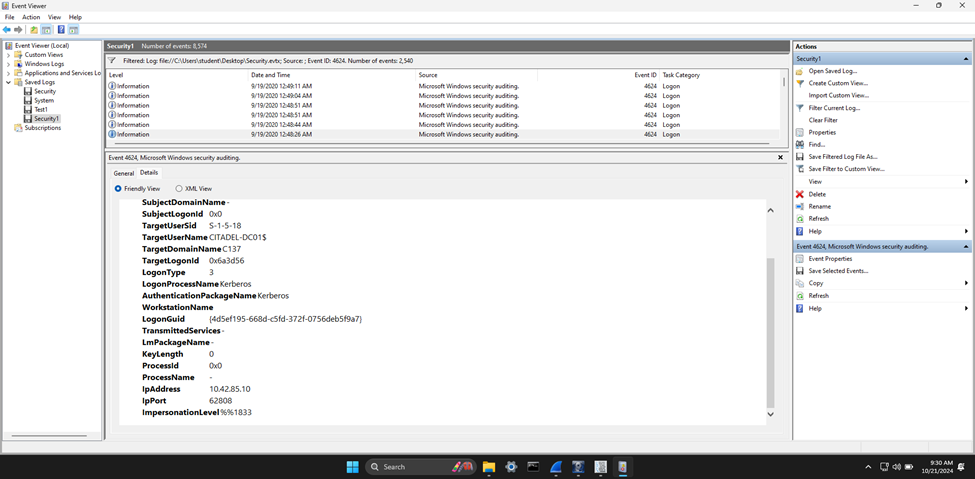
1. What was the network layout of the victim network?



LLMNR queries from the DC to the multicast address 224.0.0.252.



Successful logon events involving the DC and user machine IP addresses.



Details of Event ID 4624 indicating a successful account logon.

**Network Layout:**

* **Domain Controller (DC):** IP address 10.42.85.10, identified as “CITADEL-DC01”.
* **User Machine:** IP address 10.42.85.115, within the same subnet.

**Analysis Tools:**

* **Wireshark Captures:** Revealed LLMNR queries from the DC to the multicast address 224.0.0.252.
* **Event Viewer Logs:** Showed successful logon events involving the DC and user machine IP addresses.

This analysis confirms the victim network consisted of at least two hosts within the 10.42.85.0/24 subnet, highlighting their roles and interactions during the incident.

**References:**

James. (2021, March 25). *Case 001 – The stolen Szechuan Sauce*. DFIR Madness. https://dfirmadness.com/the-stolen-szechuan-sauce/

*Case 001 - Szechuan Sauce | Digital Forensics & Incident Response*. (n.d.). https://www.iblue.team/ctf-challenges/dfir-madness-ctf-challenges/case-001-szechuan-sauce

*Walkthrough of DFIR Madness PCAP*. (2021, July 9). [Video]. Netresec. https://www.netresec.com/?page=Blog&month=2021-07&post=Walkthrough-of-DFIR-Madness-PCAP

*MDwiki*. (n.d.). https://ericzimmerman.github.io/#!index.md

Chris. (2021, May 20). *The Case of the Missing Szechuan Sauce: investigation notes*. DEV Community. https://dev.to/evilcel3ri/the-case-of-the-missing-szechuan-sauce-investigation-notes-1di7

*VirusTotal*. (n.d.). VirusTotal. https://www.virustotal.com/gui/home/upload

The Volatility Foundation. (2024, March 11). *Volatility Training | The Volatility Foundation | Open Source Memory Forensics Framework - The Volatility Foundation - Promoting accessible memory analysis tools within the Memory Forensics community*. The Volatility Foundation - Promoting Accessible Memory Analysis Tools Within the Memory Forensics Community. https://volatilityfoundation.org/volatility-training/

*FTK Imager - Forensic Data Imaging and Preview Solution | Exterro*. (2024, April 4). Exterro. https://www.exterro.com/digital-forensics-software/ftk-imager

*Wireshark • Learn*. (n.d.). Wireshark. https://www.wireshark.org/learn

Markdefalco. (n.d.). *Event viewer*. Microsoft Learn. https://learn.microsoft.com/en-us/shows/inside/event-viewer

James. (2021a, February 1). *Case 001 PCAP Analysis*. DFIR Madness. https://dfirmadness.com/case-001-pcap-analysis/

Ananin, V., & Ananin, V. (2024, October 4). *Malware analysis in ANY.RUN: The Ultimate Guide*. ANY.RUN’s Cybersecurity Blog. https://any.run/cybersecurity-blog/malware-analysis-in-a-sandbox/