Lab Report

Name: Inor Wang

Title: Forensic Timeline Analysis w/ Timesketch

Case: 25-T107

Date: 10/31/2025

Table of Contents

Document Revision History

Name	Revision Date	Version	Description
Inor Wang	10/31/2025	0.1	Draft

Executive Summary

On 31 October 2025, examiner Inor Wang analyzed triaged Windows data from CITADEL-DC01 and DESKTOP-SDN1RPT to explain RDP, logon, and persistence activity tied to public IP 194.61.24.102 (Timesketch → Russia). Data sources were existing KAPE timelines in Timesketch, Hayabusa logonsummary-success/-failed CSVs, and Saved Searches (RDP started/ended, hostname, network shares, OS version, Defender disabled, service creation, user execution, file save/archive, Windows crash). The goal was to confirm that a burst of failed Administrator logons from a kali host led to a successful DC login, RDP pivot to the desktop, service-based persistence with cmd.exe, and staging/compression of files in C:\FileShare\Secret.

Key findings

- **Brute-force → success:** DC01 recorded 96 failed Administrator logons — 95 from kali, 1 from WIN-E0PO207ERMD — and later 4 successful Administrator logons from kali, confirming the attack eventually got valid credentials.
- **Initial RDP to DC01:** First RDP (logon type 10) to DC01 was 2020-09-19 03:21:48.891 UTC, user Administrator, domain C137, source 194.61.24.102, logged under CITADEL-DC01$, showing DC01 hosted/brokered the session.
- **Lateral to desktop:** DC01 executed Remote Desktop Connection.lnk at 03:35:33.594, followed by the first RDP (4624) to DESKTOP-SDN1RPT at 03:36:24.432, also type 10, user Administrator, domain C137 → attacker moved from DC01 to the workstation.
- **Follow-on DC01 RDPs:** Three more RDPs to DC01 ≥10 min after the first: 03:56:04.322 / .587 / .653 UTC; no comparable late RDP to the desktop.
- **Suspicious logon failures (T1110):** Four creation-time events for kali in the same window: 03:21:46.782, 03:22:07.924, 03:22:36.284, 03:56:03.152 UTC → lines up with the brute-force and later sessions.
- **Host / IP / OS / shares:** DC01 renamed mnmsrvc → CITADEL-DC01 (2020-09-18 22:46:43); desktop mnmsrvc → DESKTOP-SDN1RPT (2020-09-18 05:46:38); DC01 IP 10.42.85.10; desktop IP 10.42.85.115; DC01 = Windows Server 2012 R2 Std Eval (6.3, 9600); desktop = Windows 10 Enterprise Eval (19041); both Pacific Standard Time; DC01 shared SYSVOL, NETLOGON, and extra share FileShare.

- **Execution & persistence:** In the RDP window (03:21–03:58) there were 6 T1204 executions; after dropping .lnk, the real program was %WINDIR%\System32\cmd.exe. A cmd.exe-backed service was created on DC01 at 03:25:44.187; a nearly identical service was created on the desktop at 03:43:14.990 with cmd.exe /c echo nheyge > \\.\pipe\nheyge, start = demand, user = LocalSystem → MITRE T1543/T1569 (service-based persistence).
- **Defense evasion:** Windows Defender disabled on DESKTOP-SDN1RPT.C137.local at 03:39:45.247 (T1562.001), i.e. after RDP access and after service activity.
- **Data staging / "Secret":** Searching for "secret" showed C:\FileShare\Secret containing real-content files NoJerry.txt (25), PortalGunPlans.txt (143), Szechuan Sauce.txt (478), SECRET_beth.txt (28) (all size >0 and ≠4096). Right before the suspicious service, MRU (T1560) showed Portal_gun.png and Jessica.jpg for user mortysmith; right after, T1560.001 showed archive C:\Users\mortysmith\Documents\loot.zip at 03:46:15.269 → consistent with gathering + compressing data.
- **Country-tagged events:** Timesketch resolved 194.61.24.102 to Russia; first RDP-ended event with that tag was 03:52:46.870, two more at 03:57:41.089; Source Name for the first flagged event was Microsoft Windows RemoteDesktopServices RdpCoreTS.
- **Other event:** DC01 logged a spoolsv.exe crash at 03:29:35.000 in the same activity window.

In conclusion, data shows one continuous intrusion: kali brute-forces Administrator on CITADEL-DC01 → succeeds → RDPs into DC01 from 194.61.24.102 (Russia) → launches RDP to DESKTOP-SDN1RPT → installs cmd.exe services on both systems → disables Defender → accesses/stages C:\FileShare\Secret → creates loot.zip under mortysmith → all between 03:21–03:58 UTC. This is enough to support timeline/persistence/attribution reporting and to recommend: remove the malicious services, re-enable Defender, review/lock down FileShare/Secret, and reset Administrator/C137 credentials.

Synopsis

The instructor provided memory and disk-based triage collections for a Windows domain controller (DC01) and a workstation (DESKTOP) to determine how the systems were accessed, what accounts were used, and whether data was staged or exfiltrated during a suspected RDP-driven intrusion. Both images were mounted read-only with Arsenal Image Mounter and processed with KAPE (!SANS_Triage/KapeTriage) to create a repeatable evidence set of Windows artifacts (EVTX, registry, user activity, network/share configuration, and execution artifacts such as Prefetch/UserAssist/EvidenceOfExecution). These KAPE captures were then parsed with Hayabusa to produce logon-summary CSVs (successful vs. failed) and imported into Timesketch to answer the lab's 41 rubric questions using the built-in Saved Searches (RDP Activity, Suspicious Logon Failures, User Execution, Archived Files, Defender Disabled, and keyword "secret"). The instructor specifically asked for a step-by-step workflow with screenshots, filters, and timestamps so every answer (user, IP, hostname, file path, and RDP time window) can be traced back to the collected triage data.

Client Questions:

Hayabusa Logon Summary

1. According to the dc01 logonsummary-success output, what user connected to this system using remote desktop (10 – RemoteInteractive)
2. What is the source IP address from this connection?
3. There were three non-service accounts that logged on to this system under "3 – Network". Other than Administrator, who were the other two accounts?
4. According to the dc01 logonsummary-failed output, how many failed login attempts from the user Administrator occurred?
5. What was the source computer hostname from this activity?
6. Based on this information, what do you think occurred?]
7. According to the dc01 logonsummary-success output, does the hostname from the failed login attempts exist here?
8. Based on this information, what do you think occurred?
9. According to the dc01 logonsummary-success output, was there a remote desktop connection (10 – RemoteInteractive)? What was the user and source IP address from this activity?

10. There were several interactive sessions (2 – Interactive). Exclusing the service accounts (SYSTEM, LOCAL SERVICE, NETWORK SERVICE, UMFD-X, DWM-X), what users logged into this system?

Timesketch Analysis

11. What is the hostname from the dc01 triage timeline (Hint: Saved Searched > Info – Hostname)

12. What is the hostname from the desktop triage timeline (Hint: Saved Searches > Info – Hostname)

13. What is the IP address of the system from the dc01 triage timeline (Hint: Saved Searches > Info – Windows Network Adapter Details. Search for "IP address" in the "values" row.)

14. What is the IP address of the system from the desktop triage timeline (Hint: Saved Searches > Info – Windows Network Adapter Details. Search for "IP address" in the "values" row.)

15. What is the OS version of the system from the dc01 triage timeline (Hint: Saved Searches > Info – Windows OS Version)

16. What is the OS version of the system from the desktop triage timeline (Hint: Saved Searches > Info – Windows OS Version)

17. All Windows domain controllers have the two network file shares: SYSVOL and NETLOGON; however, this domain controller had a third. What is the name of this network file share. (Hint: Saved Searches > Info – Network Shares. Search for "ShareName" in the "values" row.)

18. What is the timezone set for both systems? (Hint: Saved Searches > Info - Timezone. Search for "TimeZoneKeyName")

In the search bar, search for the public IP address we found in the Haybusa login summary for the dc01 system. Timesketch should have resolved this IP address to a country.

19. What is the country tag and flag Timesketch is using for this IP address?

20. Skip down to the first entries where you see the flag, we see this IP address interacting with the system. What is the "Source Name" according to the entry.

In Saved Searches, click on "T1021.001-RDP Activity Started". Search the first couple of entries and find one where "timestamp_desc" is "Creation Time". Hover over this row and navigate left to the icon "Filter for value." This represents when the entries were created on the system. There should be 11 entries if you have all timelines selected. Event ID 4624 denotes "successful login" to the system.

21. What is the first date timestamp of the first 4624 entry for the dc01 system? Star this entry.

22. What is the login_type, username, and domain for this entry?

23. What is the first date timestamp of the first 4624 entry for the desktop system? Star this entry.

24. What is the login_type, username, and domain for this entry?

25. Were there additional RDP connections to the dc01 system at least 10 minutes after the initial? If so, what are the date timestamps? Star these entries if necessary.

26. Were there additional RDP connections to the desktop system at least 10 minutes after the initial? If so, what are the date timestamps? Star these entries if necessary.

In Saved Searches, click on "T1021.001-RDP Activity Ended". Search the first couple of entries and find one where "timestamp_desc" is "Creation Time". Hover over this row and navigate left to the icon "Filter for value." This represents when the entries were created on the system. There should be 41 entries if you have all timelines selected. Find the entries with the flag and country we found earlier.

27. What is the date timestamp of the first entry with the country tag we found earlier? Star this entry.

28. What are the date timestamps of all other entries with the country tag? Star these entries if necessary.

In Saved Searches, click on "T1110-Suspicious Logon Failures." Search the first couple of entries and find one where "timestamp_desc" is "Creation Time". Hover over this row and navigate left to the icon "Filter for value." This represents when the entries were created on the system. There should be 109 entries if you have all timelines selected. Search these entries for the suspicious hostname we found in the hayabusa logon summary for the dc01 system.

29. What are the date timestamp entries for the suspicious system connections? (Hint: there should be four.) Star these entries if necessary.

In Saved Searches, click on "T1204-User Execution or Shortcut." Filter all timelines with the exception of the dc01 timeline. There should be 15 entries.

30. How many entries represent the execution of an application within the RDP time window from the suspicious country's IP address?

31. Filtering out anything with a ".lnk" file extension, provide the full path of the application. This is located in the "value_name" row. Star the entries.

32. There is an entry for "Remote Desktop Connection.lnk". What is the date timestamp for this execution? Does this coincide with an RDP connection to another system we've see? If so, what system (hostname)? Star the entry.

In Saved Searches, click on "T1543-Installation or Execution of a Windows Service". At the top, click on "Add Timefilter" and create a time window that includes the start and end date timestamps for the RDP session by the suspicious country's IP address? Next, search the first couple of entries and find one where "timestamp_desc" is "Creation Time". Hover over this row and navigate left to the icon "Filter for value." This represents when the entries were created on the system. You should have 6 entries.

33. There is an application that you have seen in previous analysis. What is the name of the application and what is the date timestamp of when this service created on the dc01 system? Star the entries.

34. What is the date timestamp of when this service created on the desktop system? Star the entries.

In Saved Searches, click on “T1560 or T1083-File Save or Discovery”. Ensure all timelines are selected.

35. Right before the creation and execution of the suspicious application above, two image (picture) files were created. We know this because a MRU (Most Recently Used) entry was created in one of the users profiles. Find the entry with two entries in the “entries” row. What are the names of the images. One should be a PNG and the other a JPG.

In Saved Searches, click on “T1560.001-Archived Files”. Search the first couple of entries and find one where “timestamp_desc” is “Creation Time”. Hover over this row and navigate left to the icon “Filter for value.” This represents when the entries were created on the system. There should be 4 entries if you have all timelines selected.

36. What is the first occurring date timestamp from these events? Star the entry.

37. These entries represent an archived file being created on the system. What is the full path of the file that was created? This should start with “C:\Users\”

38. Was Windows Defender disabled on any system? If so, what system (hostname) and was date timestamp? (Hint: Saved Searches > T1562.001-Win Defender Disabled).

39. An application crashed on the dc01 system. What is the date timestamp and full path of the application that crashed? (Hint: Saved Searches > Windows Crash activity).

Finally, the client kept saying “the secret was stolen”. Search for the keyword “secret” across all timelines. Search the first couple of entries and find one where “timestamp_desc” is “Creation Time”. Hover over this row and navigate left to the icon “Filter for value.” Additionally filter on data_type “windows:lnk:link”. There should be 12 entries.

40. What is file path of the directory that contains the word “secret”?

41. Find the files that have a file size greater than 0 and not 4096. What are the file names?

Scope of Work:

- Acquisition and triage of **DC01-E01.zip** and **DESKTOP-E01.zip** (mounted via Arsenal).
- Analyzation of triage and timelines via Hayabusa and Timesketch.
- Verification of evidentiary integrity using MD5, SHA1, and SHA256 cryptographic hashes.
- All tools were run against mounted, read-only images to preserve evidentiary integrity.

Evidence Analyzed

This section provides details of the digital evidence collected

Evidence ID	**E001**
Name	DC01-E01.zip
Type	Zip archive data, at least v2.0 to extract, compression method=store
Size	4,836,649,413 bytes (4.83 GB)
MD5	E57FC636E833C5F1AB58DFACE873BBDE
SHA1	29F841501B76CE461EC1049E21D769D151246D69
SHA256	EFE06D12388DBC000FA4AE306746DDACA3893A6CDBD55311B52F5833 E717ACD9

Evidence ID	**E002**
Name	DESKTOP-E01.zip
Type	Zip archive data, at least v2.0 to extract, compression method=deflate
Size	6.37 GB
MD5	71C5C3509331F472ABCDF81EB6EFFF07
SHA1	C56B619B5A4ADD5F269FB6731543CF7BA759DB0D
SHA256	N/A (Not Provided)

Tools Used

Workstation

Hostname	Operating System	Build	Physical / Virtual	Built
IS-4523-001-WINDOWS	Windows 11	2021	Virtual	09/06/2025
IS-4523-001-GREYMHATTER	Fedora	2025	Virtual	10/31/2025

Software

Name	Version	Release	Purpose
Arsenal Image Mounter (Arsenal Recon)	3.11.307	Apr 2025	Mount the DC01 and DESKTOP disk images read-only as local disks, assign drive letters to the system volume (with Windows, Program Files, Users), and expose the file system so KAPE can target the correct mounted volume without altering evidence.
Kape (Kroll)	1.2.0.0	Jun 2025	Run the !SANS_Triage (and compare to KapeTriage) collection against the mounted volume to rapidly acquire key artifacts (e.g., Prefetch, EvidenceOfExecution, registry hives, event logs, LNK/Jumplists, user profiles) into a ZIP named DC01/DESKTOP, producing the counts, deferred/duplicate stats, and data needed to answer the rubric questions.
Hayabusa (Yamato Security)	3.6.0	2025	Parse Windows EVTX logs from the triage collection and generate CSV summaries of successful and failed logons, logon types (e.g. RDP), and other security-relevant events to support timeline analysis.
Timesketch (Google)	N/A	N/A	Ingest the collected timeline/Plaso data into a central web interface to search, filter, and tag events (e.g. RDP activity, suspicious logon failures, execution, Defender changes) and star items referenced in the report.
Plaso (Plaso)	20250918	2025	Build a unified, time-ordered super-timeline from multiple Windows artifacts (event logs, registry, LNK/UserAssist, etc.) so activity from both hosts can be reviewed and correlated in Timesketch.

Analysis Findings

Overview of Examination Procedures

The examiner mounted the provided triage collections for both systems (DC01 and DESKTOP) in a read-only manner and verified the presence of core Windows artifacts (event logs, registry hives, user profiles, and shared folders). After using gkape for DC01 and DESKTOP, the Windows event logs from the KAPE output (Windows\System32\winevt\Logs\) were parsed with Hayabusa to generate the dc01-logonsummary-successful.csv and dc01-logonsummary-failed.csv files, which were then filtered (e.g., for "10 – RemoteInteractive", "3 – Network", "kali", and Administrator failures) to identify RDP activity, non-service network logons, and brute-force behavior. The resulting timelines were imported into Timesketch, and the examiner used the built-in Saved Searches (Info – Hostname, Info – Windows Network Adapter Details, Info – Windows OS Version, Info – Network Shares, Info – Timezone, T1021.001 – RDP Activity Started/Ended, T1110 – Suspicious Logon Failures, T1204 – User Execution or Shortcut, T1560 / T1560.001 – Archived Files, T1562.001 – Win Defender Disabled) to answer the numbered questions and to star the entries referenced in the Key Findings. Public IP 194.61.24.102 and the attacker hostname kali were used as pivots to correlate failed logons, later successful logons, RDP to DC01 and DESKTOP, execution of Remote Desktop Connection.lnk, creation of loot.zip, and access to C:\FileShare\Secret\.

Additional targeted analysis was performed using:

- **Arsenal Image Mounter (Arsenal Recon)** — Mounted the DC01 and desktop evidence read-only and identified the Windows system volumes for triage.
- **KAPE / gkape (Kroll)** — Executed the !SANS_Triage compound target with Container=ZIP, Deduplicate=On, Process VSCs=Off; preserved command lines and logs for each host.
- **Hayabusa** — Parsed collected event logs to produce dc01-logonsummary-successful.csv and dc01-logonsummary-failed.csv, which were then filtered for RDP (10), network (3), Administrator failures, and the **kali** source.
- **Timesketch** — Reviewed ATT&CK-mapped Saved Searches to identify RDP sessions, suspicious logon failures, user execution, Defender tampering, archive creation, and files in C:\FileShare\Secret\; starred entries that the lab required to be marked.
- **PowerShell / quick file inspection** — Spot-verified collected artifacts and reviewed configuration/triage files when needed.

Throughout the process, all findings were documented, and starred entries in Timesketch were used to preserve the analytic trail cited in the Key Findings.

Evidence Reviewed

1. **DC01-E01.zip (E001): Windows system image (domain controller)**
2. **DESKTOP-E01.zip (E002): Windows desktop workstation image**

Key Findings

Hayabusa Logon Summary

1. According to the dc01 logonsummary-success output, what user connected to this system using remote desktop (10 – RemoteInteractive)?

- **Analysis Performed:**
  - The examiner successfully downloaded and imported the Greymhatter system.
  - The Triage captures were transferred successfully to the Greymhatter system and the examiner used Hayabusa on both captures. The examiner examined the dc01-logonsummary-successful output from the Hayabusa command.
    - Command: *hayabusa-summary kape/DC01/F/Windows/System32/winevt/logs/dc01*
  - Command: *cat dc01-logonsummary-successful.csv | grep "10 – RemoteInteractive"*
- **Answer:**
  The user connected to the DC01 system using remote desktop (10 – RemoteInteractive) was "**CITADEL-DC01$"**, as shown in Figure 1.

- **Supporting Evidence:**

```
/opt/share/hayabusa ❯ cat dc01-logonsummary-successful.csv | grep "10 - RemoteInteractive"
4,Sec 4624,Administrator,C137,CITADEL-DC01.C137.local,10 - RemoteInteractive,CITADEL-DC01$,C137,CITADEL-DC01,194.61.24.102
```

Figure 1. Outputting the line with the remote desktop connection within the dc01 logonsummary-success ("10 - RemoteInteractive")

2. What is the source IP address from this connection?

- **Analysis Performed:**
  - The examiner examined the dc01-logonsummary-successful output from the Hayabusa command.
    - Command: *hayabusa-summary kape/DC01/F/Windows/System32/winevt/logs/dc01*
  - Command: *cat dc01-logonsummary-successful.csv | grep "10 – RemoteInteractive"*
- **Answer:**
  The source IP address from the remote desktop connection (10 – RemoteInteractive) is "**194.61.24.102**", as shown in Figure 2.

- **Supporting Evidence:**

```
/opt/share/hayabusa ❯ cat dc01-logonsummary-successful.csv | grep "10 - RemoteInteractive"
4,Sec 4624,Administrator,C137,CITADEL-DC01.C137.local,10 - RemoteInteractive,CITADEL-DC01$,C137,CITADEL-DC01,194.61.24.102
```

Figure 2. Outputting the line with the remote desktop connection within the dc01 logonsummary-success ("10 - RemoteInteractive")

3. There were three non-service accounts that logged on to this system under "3 - Network". Other than Administrator, who were the other two accounts?

- **Analysis Performed:**
  - The examiner examined the dc01-logonsummary-successful output from the Hayabusa command.
    - Command: *hayabusa-summary kape/DC01/F/Windows/System32/winevt/logs/dc01*
  - Command: *cat dc01-logonsummary-successful.csv | grep "3 – Network"*
- **Answer:**
  The other two non-service accounts that logged on to the system under "3 – Network" was **"mortysmith"** and **"ricksanchez"**, as shown in Figure 3.

- **Supporting Evidence:**

```
/opt/share/hayabusa ❯ cat dc01-logonsummary-successful.csv | grep "3 - Network"
646,Sec 4624,WIN-E0PO207ERMD$,C137,WIN-E0PO207ERMD.C137.local,3 - Network,-,-,,fe80::2dcf:e660:be73:d220
499,Sec 4624,CITADEL-DC01$,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,fe80::2dcf:e660:be73:d220
414,Sec 4624,WIN-E0PO207ERMD$,C137,WIN-E0PO207ERMD.C137.local,3 - Network,-,-,,::1
314,Sec 4624,CITADEL-DC01$,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,::1
95,Sec 4624,DESKTOP-SDN1RPT$,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,10.42.85.115
73,Sec 4624,WIN-E0PO207ERMD$,C137,WIN-E0PO207ERMD.C137.local,3 - Network,-,-,,10.42.85.10
57,Sec 4624,mortysmith,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,10.42.85.115
54,Sec 4624,CITADEL-DC01$,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,10.42.85.10
48,Sec 4624,CITADEL-DC01$,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,-
33,Sec 4624,WIN-E0PO207ERMD$,C137,WIN-E0PO207ERMD.C137.local,3 - Network,-,-,,-
29,Sec 4624,Administrator,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,10.42.85.115
15,Sec 4624,ricksanchez,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,10.42.85.115
4,Sec 4624,Administrator,C137,CITADEL-DC01.C137.local,3 - Network,-,-,kali,-
4,Sec 4624,ANONYMOUS LOGON,NT AUTHORITY,WIN-E0PO207ERMD.C137.local,3 - Network,-,-,,-
3,Sec 4624,ANONYMOUS LOGON,NT AUTHORITY,CITADEL-DC01.C137.local,3 - Network,-,-,,-
3,Sec 4624,ANONYMOUS LOGON,NT AUTHORITY,WIN-E0PO207ERMD,3 - Network,-,-,,-
2,Sec 4624,ricksanchez,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,-
1,Sec 4624,ANONYMOUS LOGON,NT AUTHORITY,WIN-HRJHA99CCDO,3 - Network,-,-,,-
1,Sec 4624,DESKTOP-SDN1RPT$,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,-
1,Sec 4624,mortysmith,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,-
1,Sec 4624,DESKTOP-SDN1RPT$,C137,CITADEL-DC01.C137.local,3 - Network,-,-,DESKTOP-SDN1RPT,10.42.85.115
1,Sec 4624,Administrator,C137,CITADEL-DC01.C137.local,3 - Network,-,-,,-
```

Figure 3. Outputting the lines with the "3 – Network" connection within the dc01 logonsummary-success to find the non-service accounts

4. According to the dc01 logonsummary-failed output, how many failed login attempts from the user Administrator occurred?

- **Analysis Performed:**
  - The examiner examined the dc01-logonsummary-failed output from the Hayabusa command.
    - Command: *hayabusa-summary kape/DC01/F/Windows/System32/winevt/logs/dc01*
  - Command: *cat dc01-logonsummary-failed.csv*
- **Answer:**
  According to the dc01 logonsummary-failed output, there were **96 failed login attempts** from the user Administrator occurred, as shown in Figure 4

- **Supporting Evidence:**

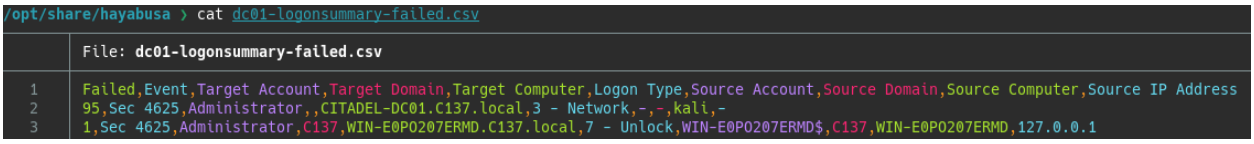


Figure 4. The output of the logonsummary-failed showing the amount of failed log ins

5. What was the source computer hostname from this activity?

- **Analysis Performed:**
  - The examiner examined the dc01-logonsummary-failed output from the Hayabusa command.
    - Command: *hayabusa-summary kape/DC01/F/Windows/System32/winevt/logs/dc01*
  - Command: *cat dc01-logonsummary-failed.csv*
- **Answer:**
  According to the dc01 logonsummary-failed output, there were two source computers that had failed log ins. The first one had 95 failed log in attempts and the source computer hostname from this activity was **kali,** as shown in Figure 5. The second one had 1 failed log in attempt and the source computer hostname from this activity was **WIN-E0PO207ERMD**, as shown in Figure 5.

- **Supporting Evidence:**

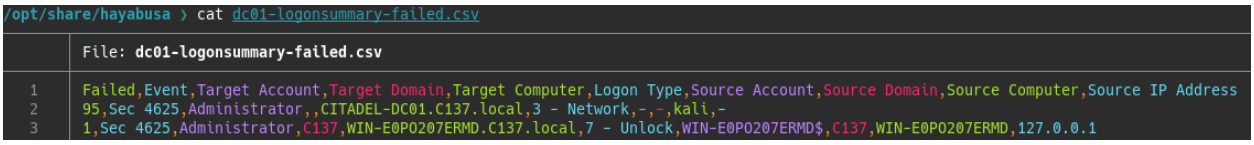


Figure 5. The output of the logonsummary-failed showing the source computer hostnames

6. Based on this information, what do you think occurred?

- **Analysis Performed:**
  - The examiner examined the dc01-logonsummary-failed output from the Hayabusa command.
    - Command: *hayabusa-summary kape/DC01/F/Windows/System32/winevt/logs/dc01*
  - Command: *cat dc01-logonsummary-failed.csv*
  - The source host named, kali, had 95 failed login attempts.
- **Answer:**
  It looks like someone on the **Kali** box was trying to log in to **CITADEL-DC01** over the network using the **Administrator** account and the attempts failed (**Password-guessing / brute-force attempt / Password Spraying against Administrator from Kali).**

- **Supporting Evidence:**

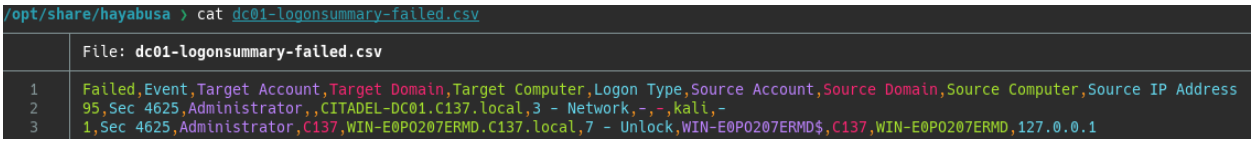


Figure 6. The output of the logonsummary-failed showing the source computer hostname and the amount of failed log ins

7. According to the dc01 logonsummary-success output, does the hostname from the failed login attempts exist here?

- **Analysis Performed:**
  - The examiner examined the dc01-logonsummary-failed output to find out that the kali machine had multiple failed login attempts.
    - Command: *cat dc01-logonsummary-failed.csv*
  - The examiner examined the dc01-logonsummary-success output and specifically filtered for the kali hostname machine.
    - Command: *cat dc01-logonsummary-successful.csv | grep "kali"*
- **Answer:**
  According to the dc01 logonsummary-success output, the kali hostname that had 95 failed login attempts **exists here**. **The machine successfully logged onto the machine with the Administrator account, 4 times**, as shown in Figure 7.

- **Supporting Evidence:**

Figure 7. Reading the output of the dc01-logonsummary-successful.csv and specifically filtered for "kali"

8. Based on this information, what do you think occurred?

- **Analysis Performed:**
  - The examiner examined the dc01-logonsummary-failed output to find out that the kali machine had multiple failed login attempts.
    - Command: *cat dc01-logonsummary-failed.csv*
  - The examiner examined the dc01-logonsummary-success output and specifically filtered for the kali hostname machine.
    - Command: *cat dc01-logonsummary-successful.csv | grep "kali"*
- **Answer:**
  It looks like someone on the Kali box was **successful in logging into CITADEL-DC01 over the network using the Administrator** using brute-force attempt / password spraying strategies, as shown in Figure 8.

- **Supporting Evidence:**

```
/opt/share/hayabusa ❯ cat dc01-logonsummary-successful.csv | grep "kali"
4,Sec 4624,Administrator,C137,CITADEL-DC01.C137.local,3 - Network,-,-,kali,-
```

Figure 8. Reading the output of the dc01-logonsummary-successful.csv and specifically filtered for "kali"

9. According to the desktop logonsummary-success output, was there a remote desktop connection (10 - RemoteInteractive)? What was the user and source IP address from this activity?

- **Analysis Performed:**
  - The examiner examined the dc01-logonsummary-success output and specifically filtered for a remote desktop connection (10 – RemoteInteractive).
    - Command: *cat dc01-logonsummary-successful.csv | grep "10 - RemoteInteractive"*
- **Answer:**
  The log entry shows a Remote Desktop (RDP) connection with logon type 10 – RemoteInteractive, where **CITADEL-DC01** appears as both the *source user* (CITADEL-DC01$) and the *target computer*. This indicates that the RDP session originated from the domain controller itself, rather than from an external workstation. The Administrator account was used, and the connection was associated with the external IP **194.61.24.102**. This suggests that the DC01 system initiated or brokered the remote session using its own machine account, which can occur when the RDP service on the domain controller authenticates the connection.

- **Supporting Evidence:**

```
/opt/share/hayabusa ❯ cat dc01-logonsummary-successful.csv | grep "10 - RemoteInteractive"
4,Sec 4624,Administrator,C137,CITADEL-DC01.C137.local,10 - RemoteInteractive,CITADEL-DC01$,C137,CITADEL-DC01,194.61.24.102
```

Figure 9. Reading the output of the dc01-logonsummary-successful.csv and specifically filtered for "10 - RemoteInteractive"

10. There were several interactive sessions (2 - Interactive). Excluding the service accounts (SYSTEM, LOCAL SERVICE, NETWORK SERVICE, UMFD-X, DWM-X), what users logged into this system?

- **Analysis Performed:**
  - The examiner examined the dc01-logonsummary-success output and specifically filtered for interactive sessions (2 – Interactive).
    - Command: *cat dc01-logonsummary-successful.csv | grep "2 - Interactive"*
- **Answer:**
  Excluding the service accounts, **the Administrator account logged in 3 times into this system with an interactive session,** as shown in Figure 10.

- **Supporting Evidence:**

```
/opt/share/hayabusa ❯ cat dc01-logonsummary-successful.csv | grep "2 - Interactive"
8,Sec 4624,DWM-1,Window Manager,WIN-E0PO207ERMD.C137.local,2 - Interactive,WIN-E0PO207ERMD$,C137,,-
8,Sec 4624,DWM-2,Window Manager,CITADEL-DC01.C137.local,2 - Interactive,CITADEL-DC01$,C137,,-
6,Sec 4624,DWM-1,Window Manager,CITADEL-DC01.C137.local,2 - Interactive,CITADEL-DC01$,C137,,-
6,Sec 4624,DWM-1,Window Manager,WIN-E0PO207ERMD,2 - Interactive,WIN-E0PO207ERMD$,WORKGROUP,,-
4,Sec 4624,Administrator,C137,CITADEL-DC01.C137.local,2 - Interactive,CITADEL-DC01$,C137,CITADEL-DC01,127.0.0.1
4,Sec 4624,Administrator,C137,WIN-E0PO207ERMD.C137.local,2 - Interactive,WIN-E0PO207ERMD$,C137,WIN-E0PO207ERMD,127.0.0.1
3,Sec 4624,Administrator,WIN-E0PO207ERMD,WIN-E0PO207ERMD,2 - Interactive,WIN-E0PO207ERMD$,WORKGROUP,WIN-E0PO207ERMD,127.0.0.1
2,Sec 4624,DWM-3,Window Manager,CITADEL-DC01.C137.local,2 - Interactive,CITADEL-DC01$,C137,,-
2,Sec 4624,DWM-1,Window Manager,WIN-HRJHA99CCDO,2 - Interactive,WIN-HRJHA99CCDO$,WORKGROUP,,-
```

Figure 10. Reading the output of dc01-logonsummary-successful.csv specifically looking for "2-Interactive"

Hayabusa Logon Summary

11. What is the hostname from the dc01 triage timeline (Hint: Saved Searches > Info - Hostname)

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on “Info - Hostname”. Then searched for the dc01 triage timeline entry that contains the hostname, as shown in Figure 11.
- **Answer:**
  The hostname from the dc01 triage timeline was changed from “mnmsrvc” to “**CITADEL-DC01**”, as shown in Figure 11.

- **Supporting Evidence:**

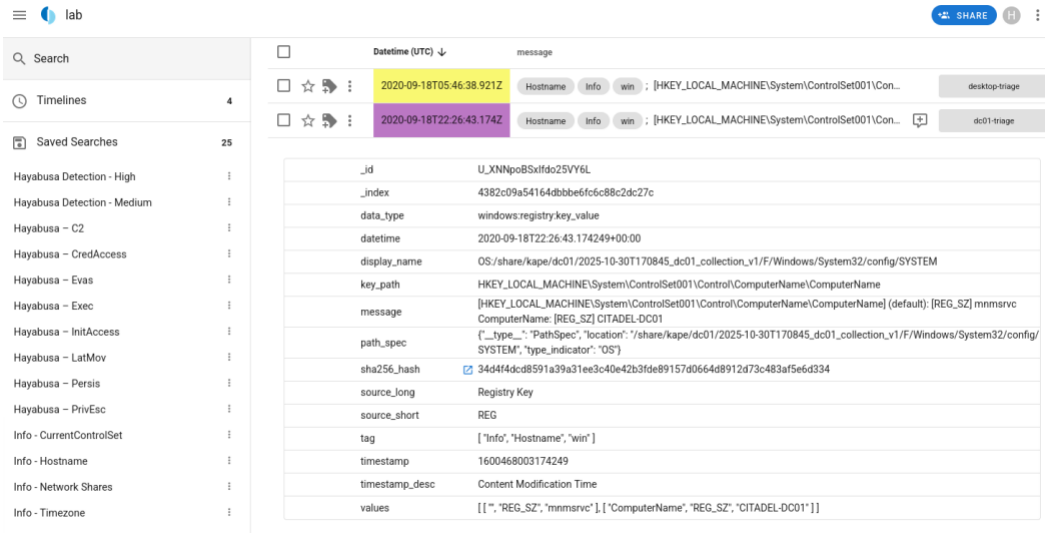


Figure 11. Hostname changed from mnmsrvc to CITADEL-DC01 on 2020-09-18 22:46:43 UTC.

12. What is the hostname from the desktop triage timeline (Hint: Saved Searches > Info - Hostname)

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "Info - Hostname". Then searched for the desktop triage timeline entry that contains the hostname, as shown in Figure 12.
- **Answer:**
  The hostname from the desktop triage timeline was changed from "mnmsrvc" to "**DESKTOP-SDN1RPT**", as shown in Figure 12.

- **Supporting Evidence:**

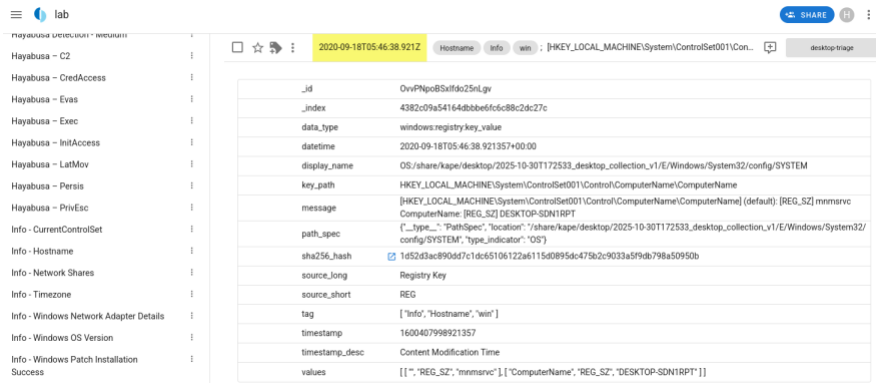


Figure 12. Hostname changed from mnmsrvc to DESKTOP-SDN1RPT on 2020-09-18 05:46:38 UTC.

13. What is the IP address of the system from the dc01 triage timeline (Hint: Saved Searches > Info - Windows Network Adapter Details. Search for "IP address" in the "values" row.)

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "Info – Windows Network Adapter Details". Then searched for the dc01 triage timeline entry that contains the IP address of the system, as shown in Figure 13.
- **Answer:**
  The IP address of the system from the dc01 triage timeline is **10.42.85.10**, as shown in Figure 13.

- **Supporting Evidence:**

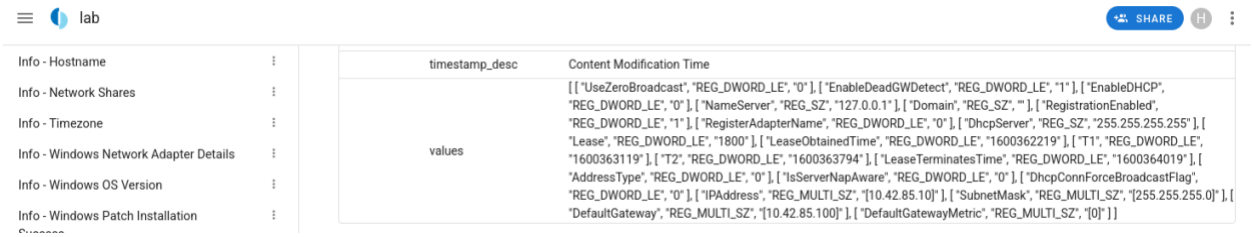


Figure 13. The system's IP address from the dc01 triage timeline is 10.42.85.10.

14. What is the IP address of the system from the desktop triage timeline (Hint: Saved Searches > Info - Windows Network Adapter Details. Search for "IP address" in the "values" row.)

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "Info – Windows Network Adapter Details". Then searched for the desktop triage timeline entry that contains the IP address of the system, as shown in Figure 14.
- **Answer:**
  The IP address of the system from the desktop triage timeline is **10.42.85.115**, as shown in Figure 14.

- **Supporting Evidence:**

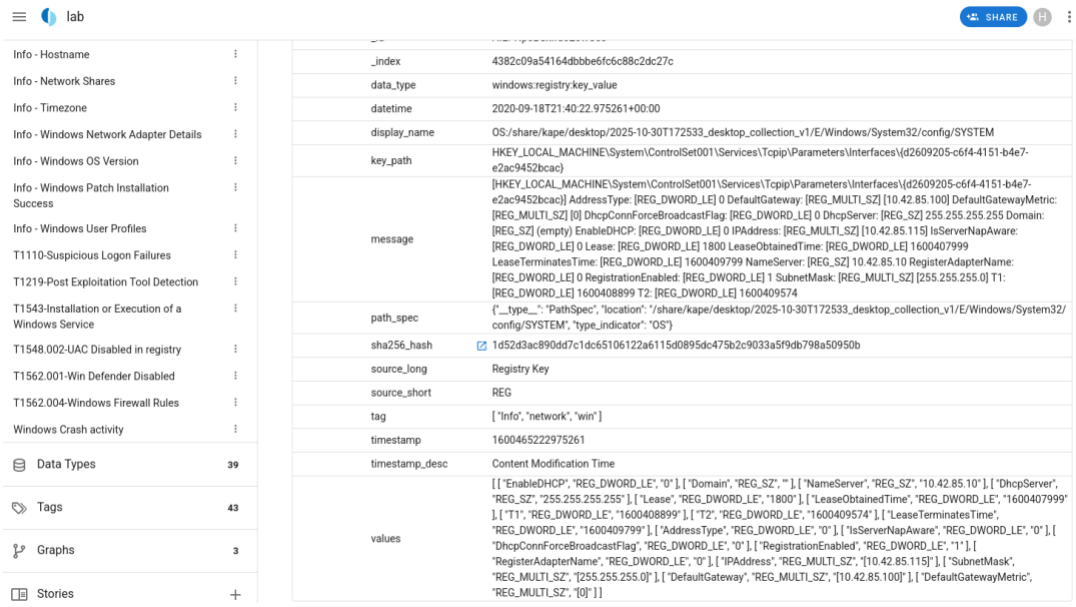
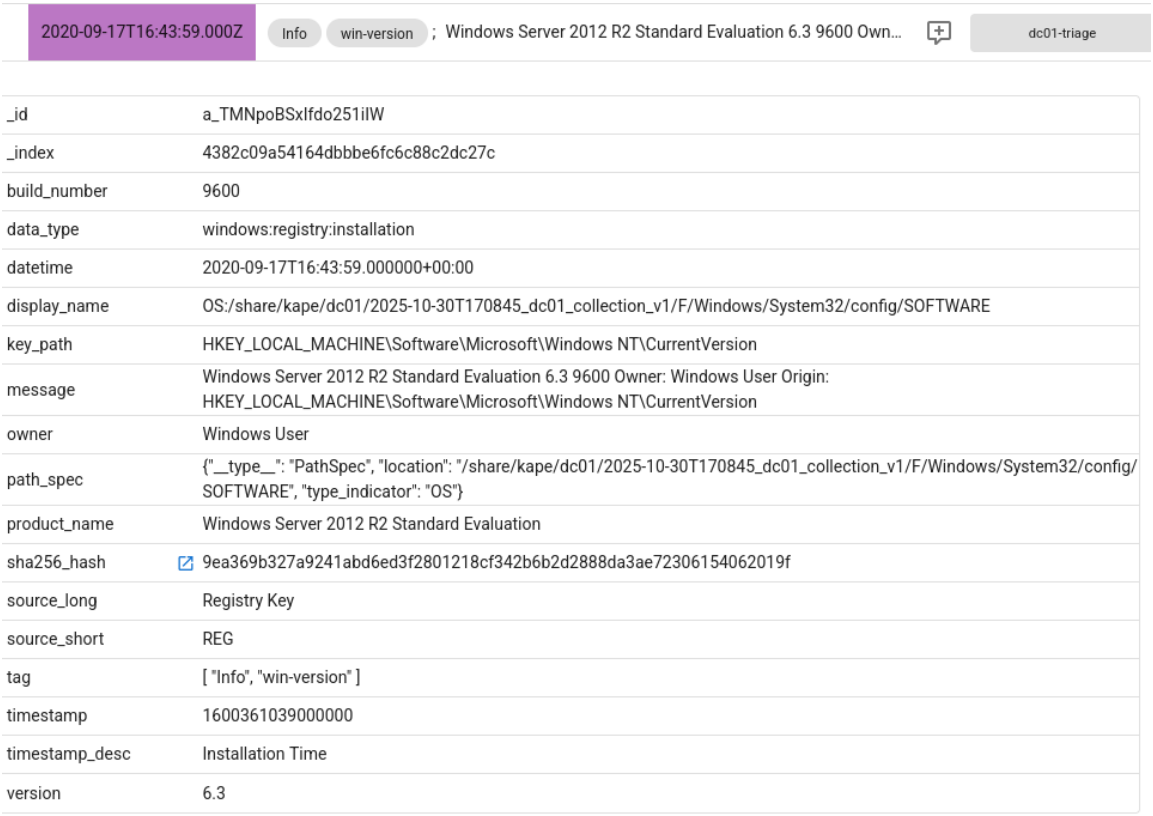


Figure 14. The system's IP address from the desktop triage timeline is 10.42.85.115

15. What is the OS version of the system from the dc01 triage timeline (Hint: Saved Searches > Info - Windows OS Version)

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on “Info – Windows OS Version”. Then searched for the dc01 triage timeline entry that contains the OS version information of the system, as shown in Figure 15.
- **Answer:**
  The system is running **Windows Server 2012 R2 Standard Evaluation (version 6.3, build 9600)**.

- **Supporting Evidence:**



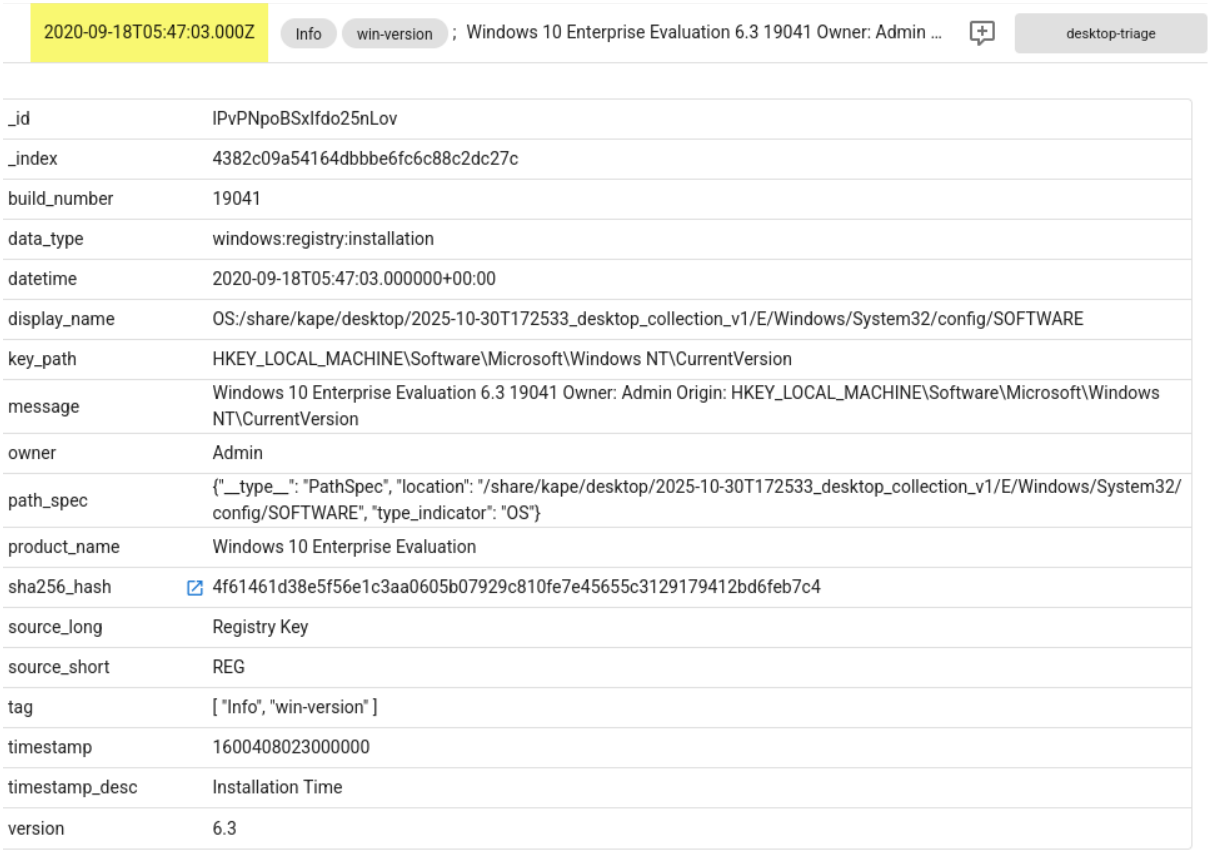
_id	a_TMNpoBSxIfdo251iIW
_index	4382c09a54164dbbbe6fc6c88c2dc27c
build_number	9600
data_type	windows:registry:installation
datetime	2020-09-17T16:43:59.000000+00:00
display_name	OS:/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Windows/System32/config/SOFTWARE
key_path	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
message	Windows Server 2012 R2 Standard Evaluation 6.3 9600 Owner: Windows User Origin: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
owner	Windows User
path_spec	{"__type__": "PathSpec", "location": "/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Windows/System32/config/SOFTWARE", "type_indicator": "OS"}
product_name	Windows Server 2012 R2 Standard Evaluation
sha256_hash	9ea369b327a9241abd6ed3f2801218cf342b6b2d2888da3ae72306154062019f
source_long	Registry Key
source_short	REG
tag	["Info", "win-version"]
timestamp	1600361039000000
timestamp_desc	Installation Time
version	6.3

Figure 15. Open view of the desktop triage timeline entry showing detailed registry data for the Windows OS version information, including product name, build number, and installation timestamp.

16. What is the OS version of the system from the desktop triage timeline (Hint: Saved Searches > Info - Windows OS Version)

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on “Info – Windows OS Version”. Then searched for the desktop triage timeline entry that contains the OS version information of the system, as shown in Figure 16.
- **Answer:**
  The system is running Windows 10 Enterprise Evaluation (version 6.3, build 19041).

- **Supporting Evidence:**



_id	IPvPNpoBSxIfdo25nLov
_index	4382c09a54164dbbbe6fc6c88c2dc27c
build_number	19041
data_type	windows:registry:installation
datetime	2020-09-18T05:47:03.000000+00:00
display_name	OS:/share/kape/desktop/2025-10-30T172533_desktop_collection_v1/E/Windows/System32/config/SOFTWARE
key_path	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
message	Windows 10 Enterprise Evaluation 6.3 19041 Owner: Admin Origin: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
owner	Admin
path_spec	{"__type__": "PathSpec", "location": "/share/kape/desktop/2025-10-30T172533_desktop_collection_v1/E/Windows/System32/config/SOFTWARE", "type_indicator": "OS"}
product_name	Windows 10 Enterprise Evaluation
sha256_hash	4f61461d38e5f56e1c3aa0605b07929c810fe7e45655c3129179412bd6feb7c4
source_long	Registry Key
source_short	REG
tag	["Info", "win-version"]
timestamp	1600408023000000
timestamp_desc	Installation Time
version	6.3

Figure 16. Open view of the dc01 triage timeline entry showing detailed registry data for the Windows OS version information, including product name, build number, and installation timestamp.

17. All Windows domain controllers have the two network file shares: SYSVOL and NETLOGON; however, this domain controller had a third. What is the name of this network file share. (Hint: Saved Searches > Info - Network Shares. Search for "ShareName" in the "values" row.)

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "Info – Network Shares". Then searched for the dc01 triage timeline entry that contains the network file shares, as shown in Figure 17.
- **Answer:**
  The name of the third network file share is **FileShare**, as shown in Figure 17.

- **Supporting Evidence:**

2020-09-18T04:49:06.826Z | Info | Network-Share | Shares | win | ; [HKEY_LOCAL_MACHINE\System\Contr... | dc01-triage

_id	qvXNNpoBSxIfdo25VYCK
_index	4382c09a54164dbbbe6fc6c88c2dc27c
data_type	windows:registry:key_value
datetime	2020-09-18T04:49:06.826030+00:00
display_name	OS:/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Windows/System32/config/SYSTEM
key_path	HKEY_LOCAL_MACHINE\System\ControlSet001\Services\LanmanServer\Shares
message	[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\LanmanServer\Shares] FileShare: [REG_MULTI_SZ] [CATimeout=0, CSCFlags=0, MaxUses=4294967295, Path=C:\FileShare, Permissions=0, Remark=, ShareName=FileShare, Type=0] NETLOGON: [REG_MULTI_SZ] [CATimeout=0, CSCFlags=4352, MaxUses=4294967295, Path=C:\Windows\SYSVOL\sysvol\C137.local\SCRIPTS, Permissions=0, Remark=Logon server share , ShareName=NETLOGON, Type=0] SYSVOL: [REG_MULTI_SZ] [CATimeout=0, CSCFlags=4352, MaxUses=4294967295, Path=C:\Windows\SYSVOL\sysvol, Permissions=0, Remark=Logon server share , ShareName=SYSVOL, Type=0]
path_spec	{"__type__": "PathSpec", "location": "/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Windows/System32/config/SYSTEM", "type_indicator": "OS"}
sha256_hash	34d4f4dcd8591a39a31ee3c40e42b3fde89157d0664d8912d73c483af5e6d334
source_long	Registry Key
source_short	REG
tag	["win", "Info", "Network-Share", "Shares"]
timestamp	1600404546826030
timestamp_desc	Content Modification Time
values	[["SYSVOL", "REG_MULTI_SZ", "[CATimeout=0, CSCFlags=4352, MaxUses=4294967295, Path=C:\\Windows\\SYSVOL\\sysvol, Permissions=0, Remark=Logon server share , ShareName=SYSVOL, Type=0]"], ["NETLOGON", "REG_MULTI_SZ", "[CATimeout=0, CSCFlags=4352, MaxUses=4294967295, Path=C:\\Windows\\SYSVOL\\sysvol\\C137.local\\SCRIPTS, Permissions=0, Remark=Logon server share , ShareName=NETLOGON, Type=0]"], ["FileShare", "REG_MULTI_SZ", "[CATimeout=0, CSCFlags=0, MaxUses=4294967295, Path=C:\\FileShare, Permissions=0, Remark=, ShareName=FileShare, Type=0]"]]

Figure 17. Open tab of the dc01 triage timeline entry displaying registry details under LanmanServer\Shares, showing information about network share configurations such as NETLOGON, SYSVOL, and FileShare entries.

18. What is the timezone set for both systems? (Hint: Saved Searches > Info - Timezone. Search for "TimeZoneKeyName")

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "Info – Timezone". Then searched for the dc01 and desktop triage timeline entry that contains the timezone information, as shown in Figure 18.
- **Answer:**
  The timezone that is set for both systems is **Pacific Standard Time**, as shown in Figure 18.

- **Supporting Evidence:**

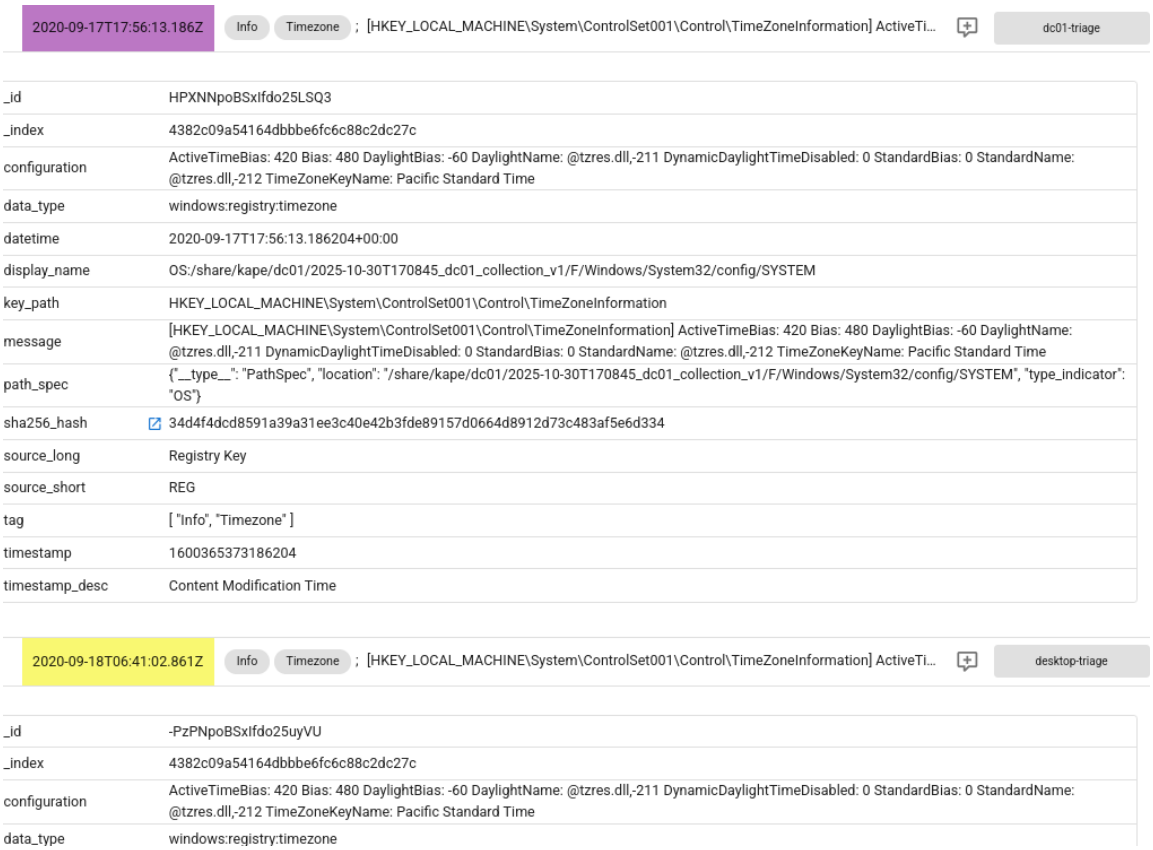


Figure 18. Displayed view of timezone configuration entries from both dc01 and desktop triage timelines, showing registry key details under TimeZoneInformation that list the TimeZoneKeyName and related daylight bias settings.

19. What is the country tag and flag Timesketch is using for this IP address?

- **Analysis Performed:**
  - The examiner used the search bar to search for the public IP address that he found in the Hayabusa login summary for the dc01 system which was 194.61.24.102**.**
  - Timesketch should have resolved the IP address to a country and displayed it's flag and tag.
- **Answer:**
  The country tag and flag that Timesketch is using for the IP address, 194.61.24.102, is **Russia**, as shown in Figure 19.

- **Supporting Evidence:**

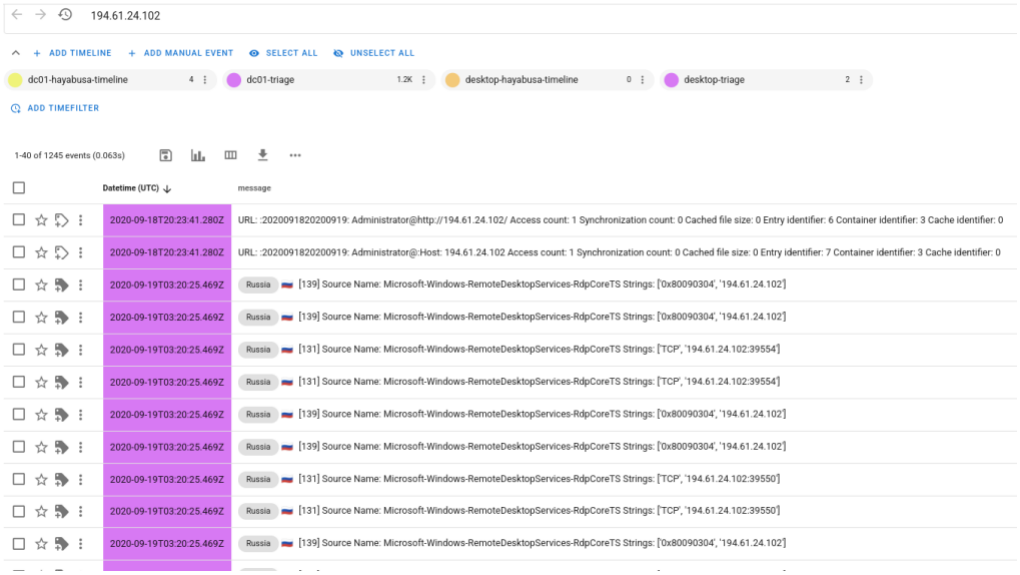


Figure 19. Search results in Timesketch showing events linked to the public IP address 194.61.24.102, which Timesketch automatically resolved and tagged with its country flag and location metadata in the event list

20. Skip down to the first entries where you see the flag, we see this IP address interacting with the system. What is the "Source Name" according to the entry.

- **Analysis Performed:**
  - The examiner examined the first entry where Timesketch assigned the Russian flag. It is interacting with the system and displays some information, as shown in Figure 20.
- **Answer:**
  The Source name according to the entry (the first entry where the Russian flag is displayed) is **Microsoft Windows RemoteDesktopServices RdpCoreTS**, as shown in Figure 20.

- **Supporting Evidence:**

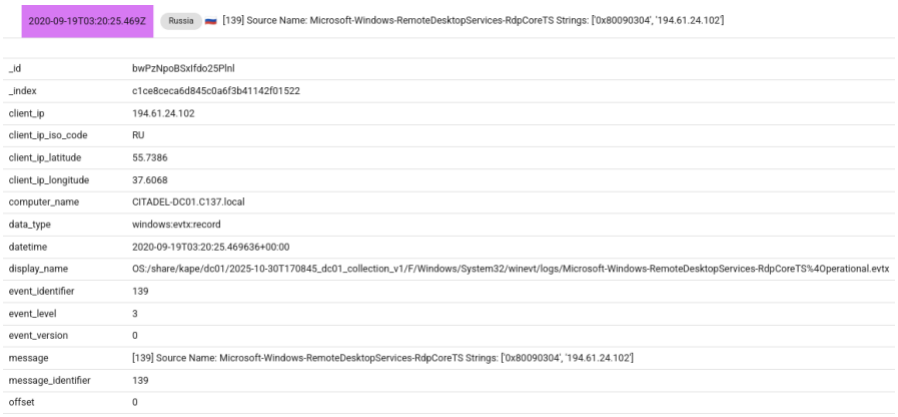


Figure 20. Expanded view of the first flagged event entry showing the IP address interaction details. The entry lists the Source Name under the Windows event log section for Remote Desktop Services (RdpCoreTS).

21. What is the first date timestamp of the first 4624 entry for the dc01 system? Star this entry.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1021.001-RDP Activity Started". Then searched the first couple of entries and found one where "timestamp_desc" is "Creation Time", filtered for this value, and found 11 entries, as shown in Figure 21.
  - The examiner starred the first 4624 entry for the dc01 system.
- **Answer:**
  The first date timestamp of the first 4624 entry for the dc01 system is **2020-09-19 03:21:48 (891 ms) UTC,** as shown in Figure 21.

- **Supporting Evidence:**

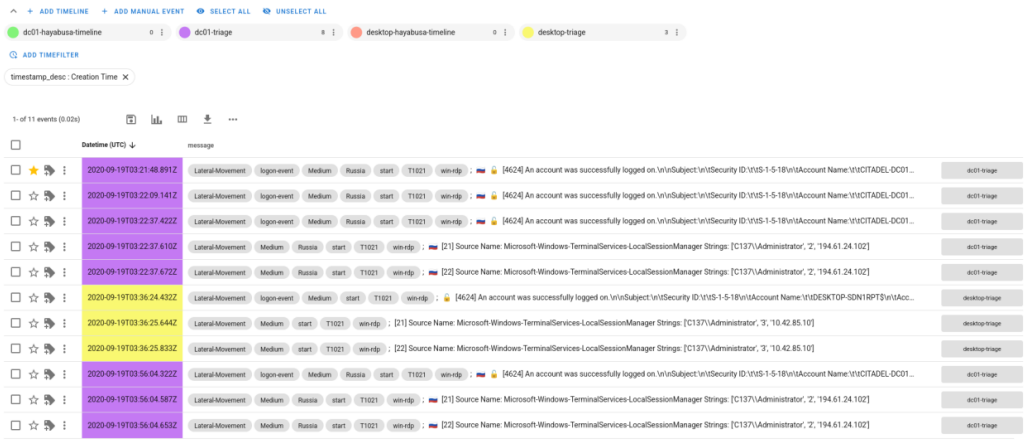


Figure 21. Timesketch view showing RDP login events after filtering for entries where "timestamp_desc" is "Creation Time"

22. What is the login_type, username, and domain for this entry?

- **Analysis Performed:**
  - After sorting for entries where “timestamp_desc” is “Creation Time”, the examiner expanded the first 4624 entry for the dc01 system, as shown in Figures 22 and 23.
  - From this expanded panel, it displays information that could prove beneficial for a digital forensics professional.
- **Answer:**
  The login_type is **10**, the username is **Administrator**, and the domain is **C137** for this entry, as shown in Figures 22 and 23.

- **Supporting Evidence:**

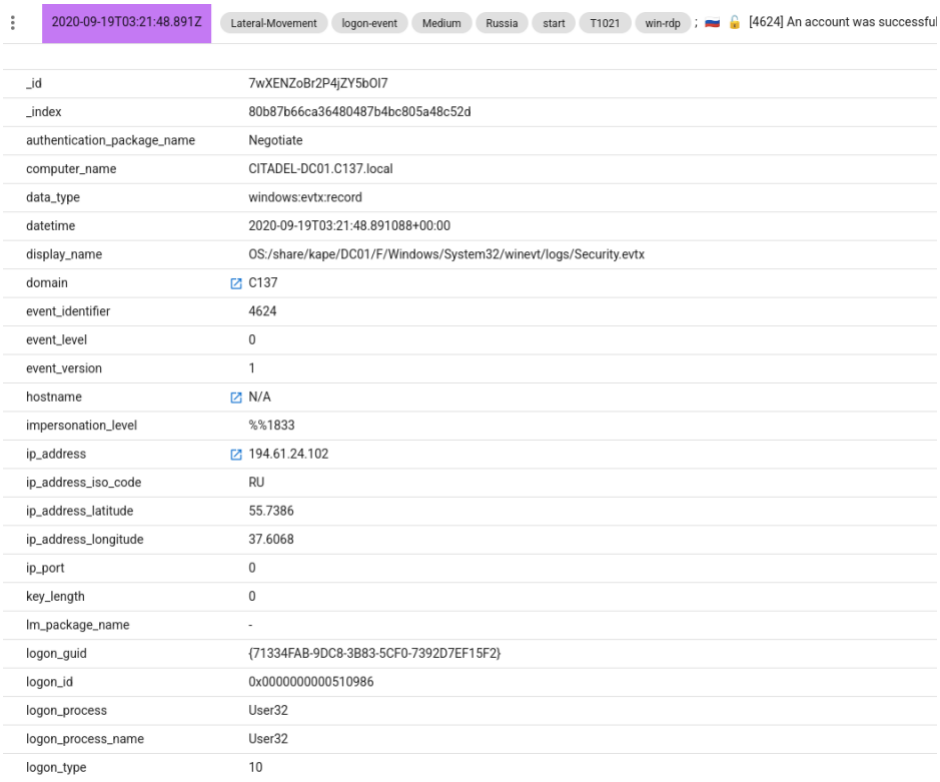


Figure 22. Timesketch event showing the first successful RDP logon (Event ID 4624) to DC01 from Russian IP 194.61.24.102 on Sept 19 2020.

Figure 23. Timesketch event showing the first successful RDP logon onto the Administrator account (Event ID 4624) created on Sept 19 2020 — Domain C137

23. What is the first date timestamp of the first 4624 entry for the desktop system? Star this entry.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on “T1021.001-RDP Activity Started”. Then searched the first couple of entries and found one where “timestamp_desc” is “Creation Time”, filtered for this value, and found 11 entries, as shown in Figure 24.
  - The examiner starred the first 4624 entry for the desktop system.
- **Answer:**
  The first date timestamp of the first 4624 entry for the desktop system is **2020-09-19 03:36:24 (432 ms) UTC,** as shown in Figure 24.

- **Supporting Evidence:**

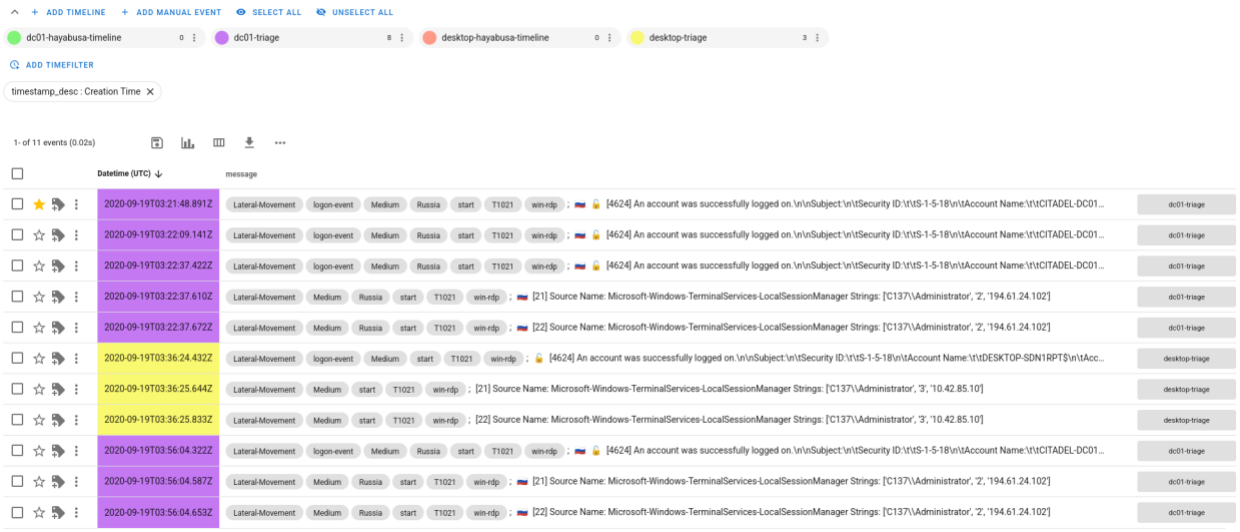


Figure 24. Timesketch view showing RDP login events after filtering for entries where “timestamp_desc” is “Creation Time”

24. What is the login_type, username, and domain for this entry?

- **Analysis Performed:**
  - After sorting for entries where "timestamp_desc" is "Creation Time", the examiner expanded the first 4624 entry for the desktop system, as shown in Figures 25 and 26.
  - From this expanded panel, it displays information that could prove beneficial for a digital forensics professional.
- **Answer:**
  The login_type is **10**, the username is **Administrator**, and the domain is **C137** for this entry, as shown in Figures 25 and 26.

- **Supporting Evidence:**

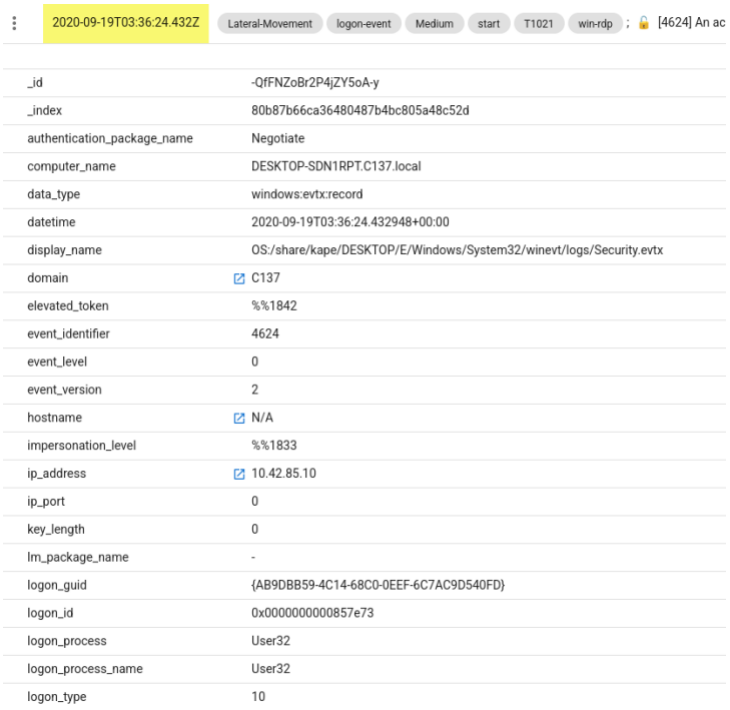


Figure 25. Timesketch event showing successful RDP logon (Event ID 4624) to DESKTOP-SDN1RPT from 10.42.85.10 on Sept 19 2020

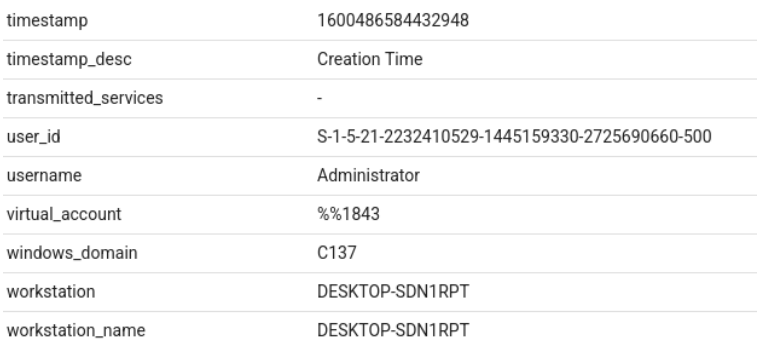


Figure 26. Timesketch event showing the first successful RDP logon onto the Administrator account(Event ID 4624) to DESKTOP-SDN1RPT from 10.42.85.10 on Sept 19 2020

25. Were there additional RDP connections to the dc01 system at least 10 minutes after the initial? If so, what are the date timestamps? Star these entries if necessary.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1021.001-RDP Activity Started". Then searched the first couple of entries and found one where "timestamp_desc" is "Creation Time", filtered for this value, and found 11 entries, as shown in Figure 27.
  - The examiner starred the three 4624 entries for the desktop system that occurred at least 10 minutes after the initial.
- **Answer:**
  There were **three additional RDP connections** to the dc01 system at least 10 minutes after the initial. The first connection's date timestamp was **2020-09-19 03:56:04 (322ms) UTC**, the second connection's date timestamp was **2020-09-19 03:56:04 (587ms) UTC**, and the third connection's date timestamp was **2020-09-19 03:56:04 (653ms) UTC**, as shown in Figure 27.

- **Supporting Evidence:**

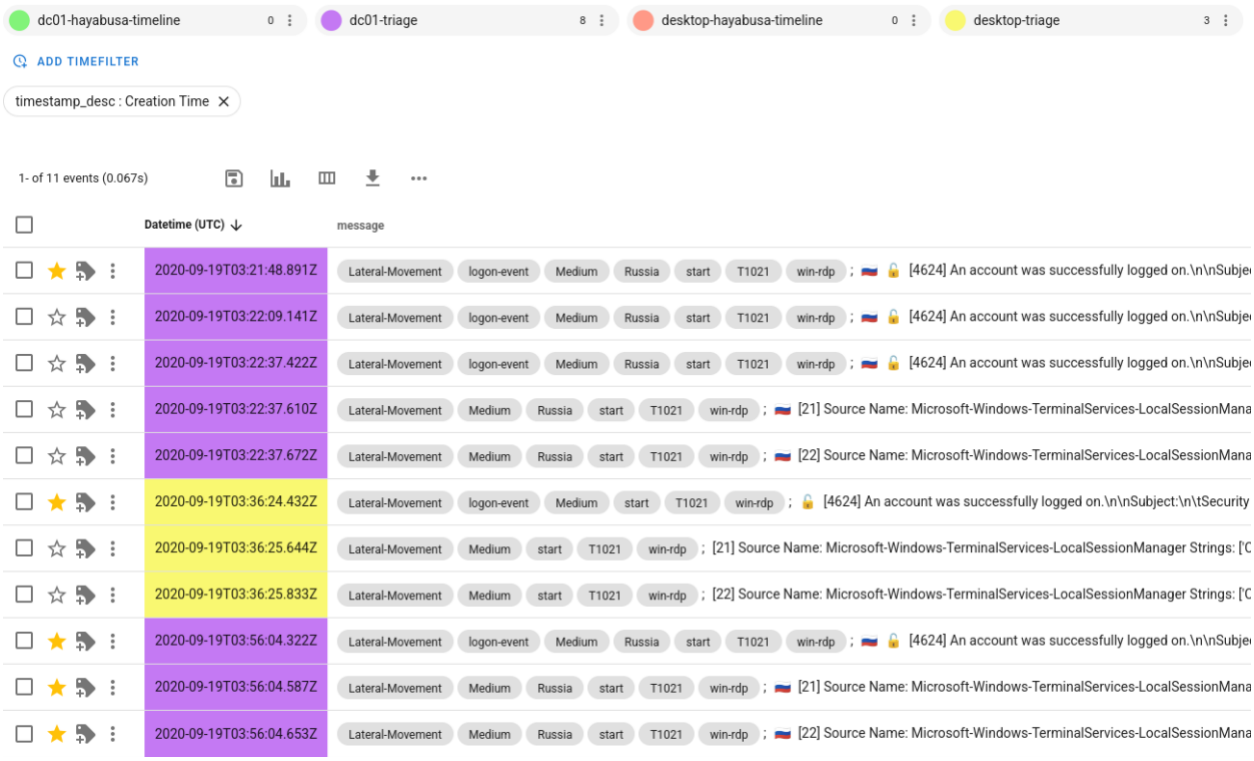


Figure 27. Starred the three additional RDP connections to the dc01 system at least 10 minutes after the initial

26. Were there additional RDP connections to the desktop system at least 10 minutes after the initial? If so, what are the date timestamps? Star these entries if necessary.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1021.001-RDP Activity Started". Then searched the first couple of entries and found one where "timestamp_desc" is "Creation Time", filtered for this value, and found 11 entries, as shown in Figure 28.
- **Answer:**
  There were **no additional RDP connections** to the desktop system at least 10 minutes after the initial, as shown in Figure 28

- **Supporting Evidence:**

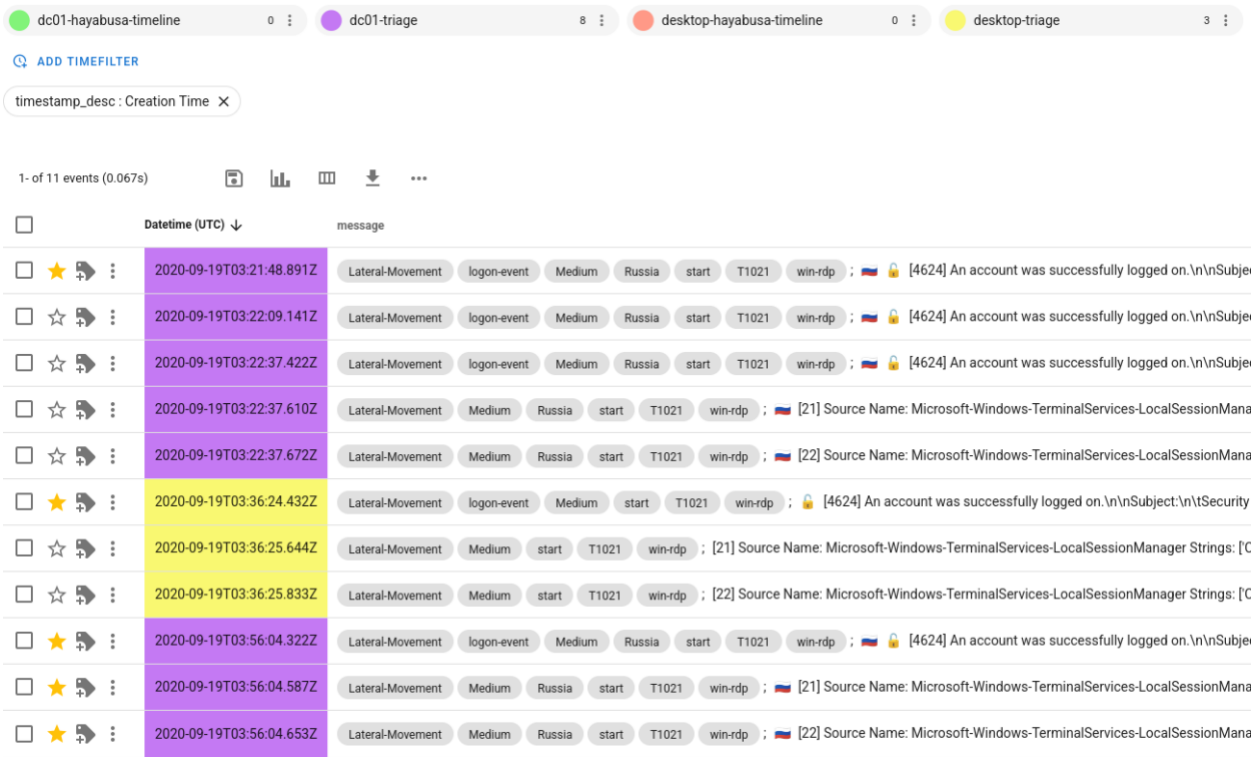


Figure 28. Filtered Timesketch view displaying RDP logon events for the desktop system. Entries are timestamped to help identify any additional remote connections occurring at least 10 minutes after the initial logon, with starred rows marking those later connect

27. What is the date timestamp of the first entry with the country tag we found earlier? Star this entry.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1021.001-RDP Activity Ended". Then searched for the first entry with the country tag of Russia, as shown in Figure 29.
- **Answer:**
  The date timestamp of the first entry with the Russia country tag is **2020-09-19 03:52:46 (870ms) UTC**, as shown in Figure 29.

- **Supporting Evidence:**

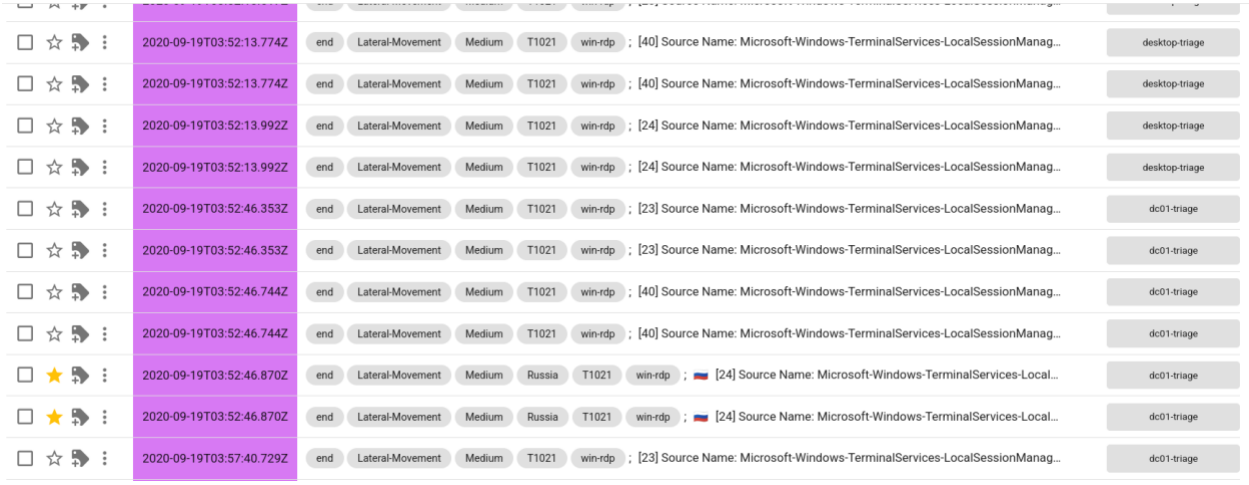


Figure 29. Filtered RDP session end events under "T1021.001-RDP Activity Ended" showing multiple timeline sources. The first entry containing the country flag tag (Russia) has been starred to mark its timestamp for analysis.

28. What are the date timestamps of all other entries with the country tag? Star these entries if necessary.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1021.001-RDP Activity Ended". Then searched for all of the entries besides the first entry with the country tag of Russia, as shown in Figures 30 and 31.
- **Answer:**
  The date timestamp of the first entry (besides the very first one) was **2020-09-19 03:52:46 (870ms) UTC**, the date timestamp of the second entry was **2020-09-19 03:57:41 (089ms) UTC**, and the date timestamp of the third entry was **2020-09-19 03:57:41 (089ms) UTC**, as shown in Figures 30 and 31.

- **Supporting Evidence:**

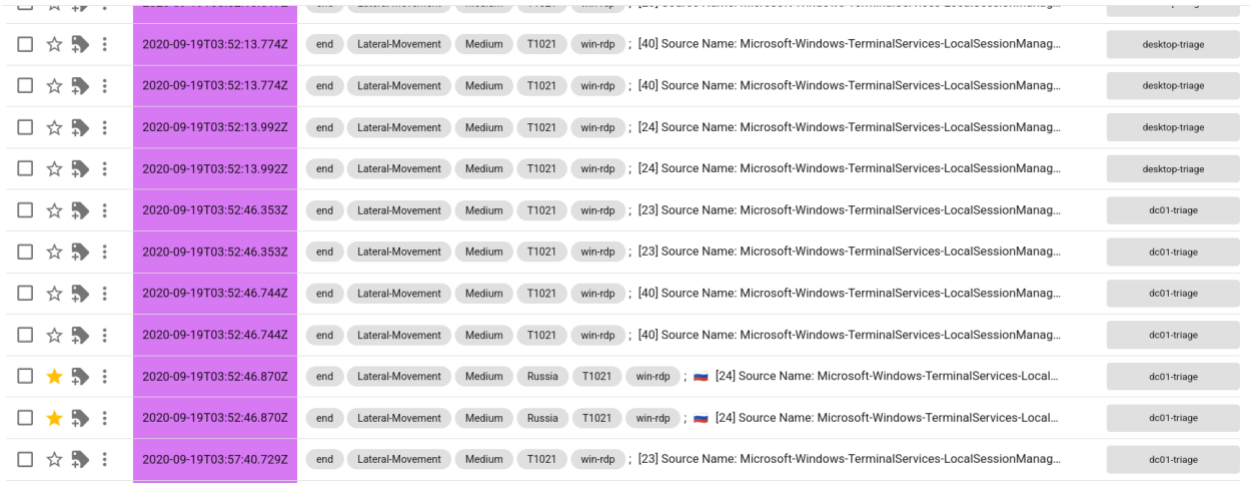


Figure 30. Filtered RDP session end events under "T1021.001-RDP Activity Ended" showing multiple timeline sources containing the Russia tag

Figure 31. Filtered RDP session end events under "T1021.001-RDP Activity Ended" showing multiple timeline sources containing the Russia tag

29. What are the date timestamp entries for the suspicious system connections? (Hint: there should be four.) Star these entries if necessary.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1110-Suspicious Logon Failures". Then searched the first couple of entries and found one where "timestamp_desc" is "Creation Time", filtered for this value, and found 109 entries, as shown in Figure 32.
  - The examiner then searched for the suspicious hostname that he found in the Hayabusa logon summary for the dc01 system which was "kali".
- **Answer:**
  The date timestamp entries for the suspicious system connections are: first one is **2020-09-19 03:21:46 (782ms) UTC**, the second one is **2020-09-19 03:22:07 (924ms) UTC,** the third one is **2020-09-19 03:22:36 (284ms) UTC**, and the last one is **2020-09-19 03:56:03 (152ms) UTC,** as shown in Figure 32.

- **Supporting Evidence:**

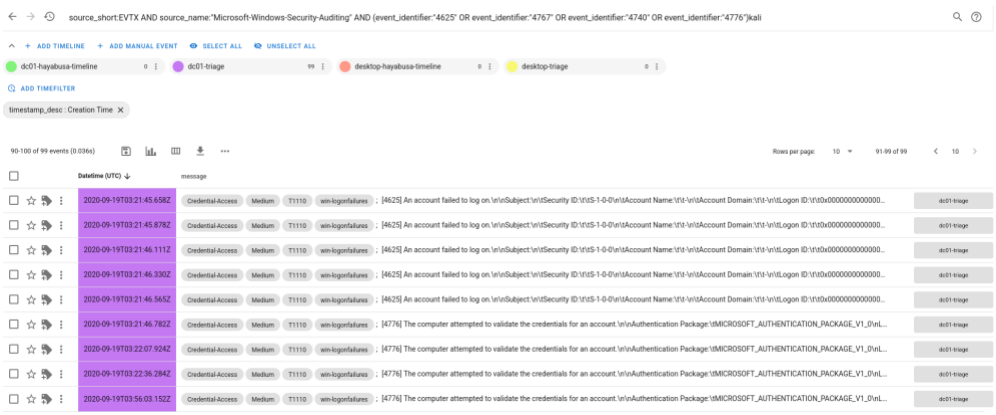


Figure 32. "Timesketch view of four suspicious failed logon attempts (T1110) from the attacker hostname to DC01 on Sept 19 2020.

30. How many entries represent the execution of an application within the RDP time window from the suspicious country's IP address?

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1204 – User Execution or Shortcut". Then filtered all timelines with the exception of the dc01 timeline.
  - The examiner then filtered for the entries within the RDDP time window from the suspicious country's IP address which was 2020-09-19 03:21:00 to 2020-09-19 03:58:00, as shown in Figure 33.
- **Answer:**
  There are **6 entries that represent the execution of an application** within the RDP time window from the suspicious country's IP address, as shown in Figure 33.

- **Supporting Evidence:**

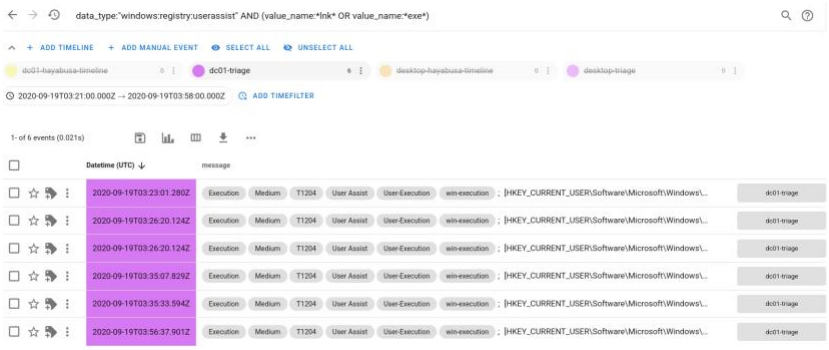


Figure 33. Filtered T1204 – User Execution or Shortcut view showing six execution entries from the dc01 triage timeline within the RDP activity window (03:21–03:58 UTC) linked to the suspicious Russian IP.

31. Filtering out anything with a ".lnk" file extension, provide the full path of the application. This is located in the "value_name" row. Star the entries.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1204 – User Execution or Shortcut". Then filtered all timelines with the exception of the dc01 timeline.
  - The examiner then filtered for the entries within the RDDP time window from the suspicious country's IP address which was 2020-09-19 03:21:00 to 2020-09-19 03:58:00, as shown in Figure 33.
  - The examiner then filtered out anything with a ".lnk" file extension and found the cmd.exe application, as shown in Figure 34.
- **Answer:**
  The full path of the cmd.exe application is **%WINDIR%\System32\cmd.exe**, as shown in Figure 34.

- **Supporting Evidence:**

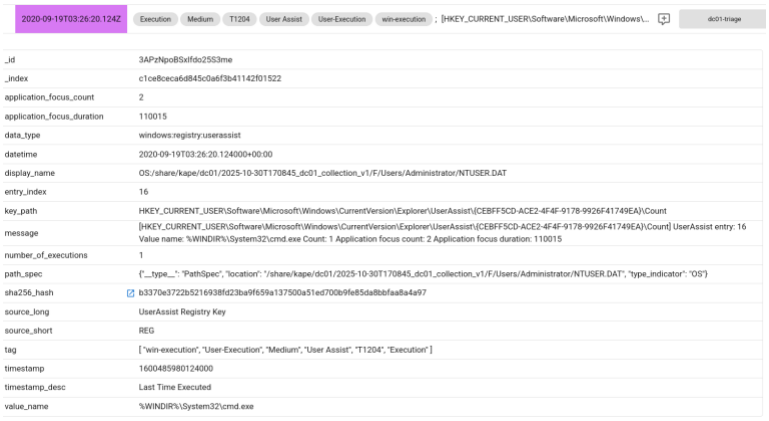


Figure 34. Expanded T1204 – User Execution or Shortcut entry from the dc01 triage timeline, showing a UserAssist registry record of cmd.exe execution by the Administrator account, including the last execution time and focus duration.

32. There is an entry for "Remote Desktop Connection.lnk". What is the date timestamp for this execution? Does this coincide with an RDP connection to another system we've see? If so, what system (hostname)? Star the entry.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1204 – User Execution or Shortcut". Then filtered all timelines with the exception of the dc01 timeline.
  - The examiner then filtered for the entries within the RDDP time window from the suspicious country's IP address which was 2020-09-19 03:21:00 to 2020-09-19 03:58:00, as shown in Figure 33.
  - The examiner then filtered for the "Remote Desktop Connection.lnk" entry, as shown in Figure 35.
- **Answer:**
  The date timestamp for this "Remote Desktop Connection.lnk" entry is **2020-09-19 03:35:33 (594ms) UTC,** as shown in Figure 35.

- **Supporting Evidence:**

2020-09-19T03:35:33.594Z | Execution | Medium | T1204 | User Assist | User-Execution | win-execution ; [HKEY_CURRENT_USER\Software\Microsoft\Windows\... | dc01-triage

_id	agPzNpoBSxlfdo25S3yf
_index	c1ce8ceca6d845c0a6f3b41142f01522
application_focus_count	0
application_focus_duration	1
data_type	windows:registry:userassist
datetime	2020-09-19T03:35:33.594000+00:00
display_name	OS:/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Users/Administrator/NTUSER.DAT
entry_index	7
key_path	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count
message	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count] UserAssist entry: 7 Value name: {%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Remote Desktop Connection.lnk Count: 1 Application focus count: 0 Application focus duration: 1
number_of_executions	1
path_spec	{"__type__": "PathSpec", "location": "/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Users/Administrator/NTUSER.DAT", "type_indicator": "OS"}
sha256_hash	b3370e3722b5216938fd23ba9f659a137500a51ed700b9fe85da8bbfaa8a4a97
source_long	UserAssist Registry Key
source_short	REG
tag	["win-execution", "User-Execution", "Medium", "User Assist", "T1204", "Execution"]
timestamp	1600486533594000
timestamp_desc	Last Time Executed
value_name	{%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Remote Desktop Connection.lnk

Figure 35. Entry showing execution of Remote Desktop Connection.lnk from the UserAssist registry key on the dc01 triage timeline, recorded at 2020-09-19 03:35:33 UTC. This timestamp coincides with the RDP connection to DESKTOP-SDN1RPT, confirming user-initiated

33. There is an application that you have seen in previous analysis. What is the name of the application and what is the date timestamp of when this service created on the dc01 system? Star the entries.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1204 – User Execution or Shortcut". Then filtered all timelines with the exception of the dc01 timeline.
  - The examiner then filtered for the entries within the RDDP time window from the suspicious country's IP address which was 2020-09-19 03:21:00 to 2020-09-19 03:58:00, as shown in Figure 33.
  - The examiner then starred the first entry of whenever the application (cmd.exe) first executed, as shown in Figure 36.
- **Answer:**
  The name of the application is "**cmd.exe"** and the date timestamp of when this service created on the dc01 system was **2020-09-19 03:25:44 (187ms) UTC**, as shown in Figure 36.

- **Supporting Evidence:**

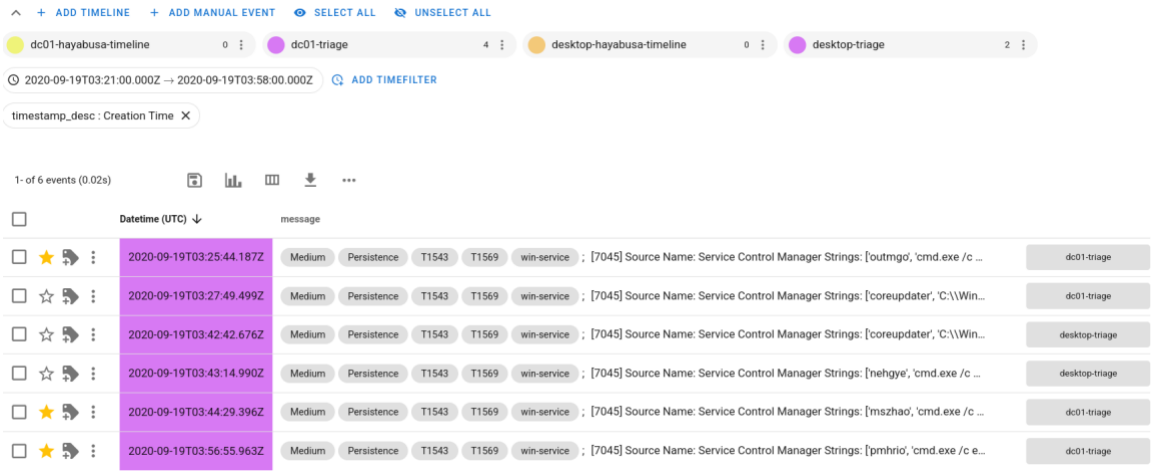
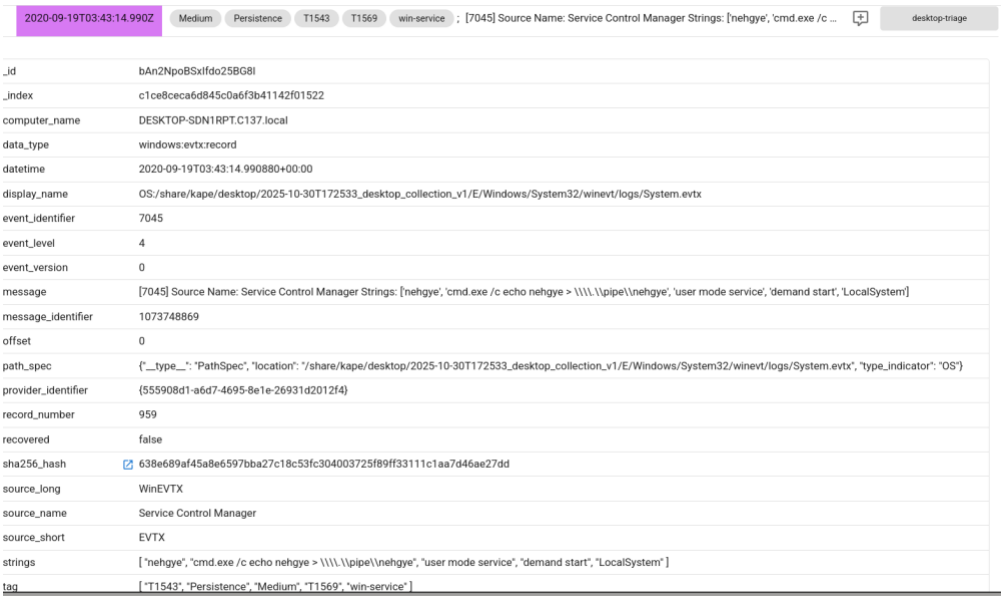


Figure 36. Filtered T1543 – Installation or Execution of a Windows Service results showing six service creation events within the RDP activity window. The starred entries indicate the creation of the cmd.exe-based service on the dc01 system, matching the applicat

34. What is the date timestamp of when this service created on the desktop system? Star the entries.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1543 – Installation or Execution of a Windows Service". Then searched for the service (cmd.exe) that was created on the desktop and was seen in previous analysis, as shown in Figure 37.
- **Answer:**
  The date timestamp of when this service created on the desktop system is **2020-09-19 03:43:14 (990ms) UTC**, as shown in Figure 37.

- **Supporting Evidence:**



2020-09-19T03:43:14.990Z	Medium Persistence T1543 T1569 win-service ; [7045] Source Name: Service Control Manager Strings: ['nehgye', 'cmd.exe /c ... desktop-triage
_id	bAn2NpoBSxIfdo25BG8I
_index	c1ce8ceca6d845c0a6f3b41142f01522
computer_name	DESKTOP-SDN1RPT.C137.local
data_type	windows:evtx:record
datetime	2020-09-19T03:43:14.990880+00:00
display_name	OS:/share/kape/desktop/2025-10-30T172533_desktop_collection_v1/E/Windows/System32/winevt/logs/System.evtx
event_identifier	7045
event_level	4
event_version	0
message	[7045] Source Name: Service Control Manager Strings: ['nehgye', 'cmd.exe /c echo nehgye > \\\\.\\pipe\\nehgye', 'user mode service', 'demand start', 'LocalSystem']
message_identifier	1073748869
offset	0
path_spec	{"__type__": "PathSpec", "location": "/share/kape/desktop/2025-10-30T172533_desktop_collection_v1/E/Windows/System32/winevt/logs/System.evtx", "type_indicator": "OS"}
provider_identifier	{555908d1-a6d7-4695-8e1e-26931d2012f4}
record_number	959
recovered	false
sha256_hash	638e689af45a8e6597bba27c18c53fc304003725f89ff33111c1aa7d46ae27dd
source_long	WinEVTX
source_name	Service Control Manager
source_short	EVTX
strings	["nehgye", "cmd.exe /c echo nehgye > \\\\.\\pipe\\nehgye", "user mode service", "demand start", "LocalSystem"]
tag	["T1543", "Persistence", "Medium", "T1569", "win-service"]

Figure 37. Event 7045 – Service Control Manager recorded a service install: cmd.exe /c echo nheyge > \\.\pipe\nheyge, set as "user mode service," start type "demand," running as LocalSystem (persistence via service, T1543/T1569).

35. Right before the creation and execution of the suspicious application above, two image (picture) files were created. We know this because a MRU (Most Recently Used) entry was created in one of the users profiles. Find the entry with two entries in the "entries" row. What are the names of the images. One should be a PNG and the other a JPG.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1560 – File Save or Discovery". Then searched for the the entry with two entries in the "entries" row that contained two images, as shown in Figure 38.
- **Answer:**
  The name of the first image is **Portal_gun.png** and the name of the second image is **Jessica.jpg**, as shown in Figure 38.

- **Supporting Evidence:**

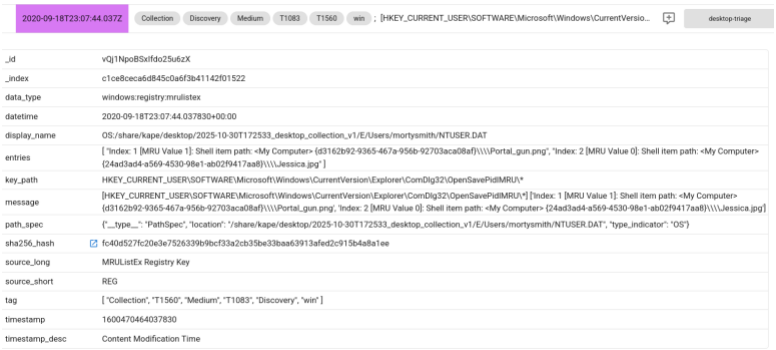


Figure 38. Expanded T1560 – File Save or Discovery entry from the desktop triage timeline, showing a MRUListEx registry record containing two image files — Portal_gun.png and Jessica.jpg — recently accessed by the user mortysmith.

36. What is the first occurring date timestamp from these events? Star the entry.

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1560.001 – Archived Files". Then searched the first couple of entries and found one where "timestamp_desc" is "Creation Time", filtered for this value, and found 4 entries, as shown in Figure 39.
- **Answer:**
  The first occurring date timestamp for these events is **2020-09-19 03:46:15 (269ms) UTC**, as shown in Figure 39.

- **Supporting Evidence:**

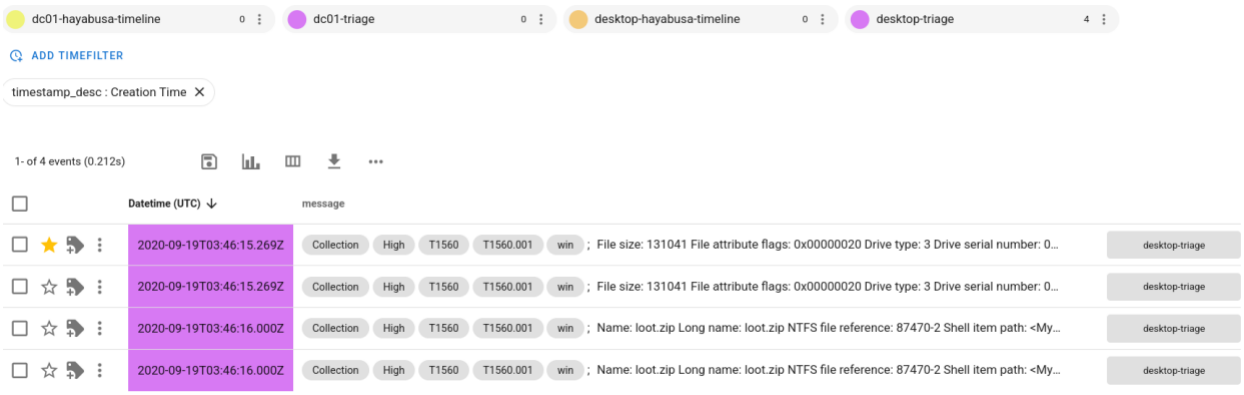


Figure 39. Filtered T1560.001 – Archived Files results displaying four archive creation events across timelines. The first occurrence, starred in the list, shows the archive file creation at 2020-09-19 03:46:15 UTC.

37. These entries represent an archived file being created on the system. What is the full path of the file that was created? This should start with "C:\Users\"

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1560.001 – Archived Files". Then searched the first couple of entries and found one where "timestamp_desc" is "Creation Time", filtered for this value, and found 4 entries, as shown in Figure 40.
  - The examiner expanded the first entry and it shows the information, as shown in Figure 40.
- **Answer:**
  The full path of the archived file that was created on the system was **C:\Users\mortysmith\Documents\loot.zip**, as shown in Figure 40

- **Supporting Evidence:**

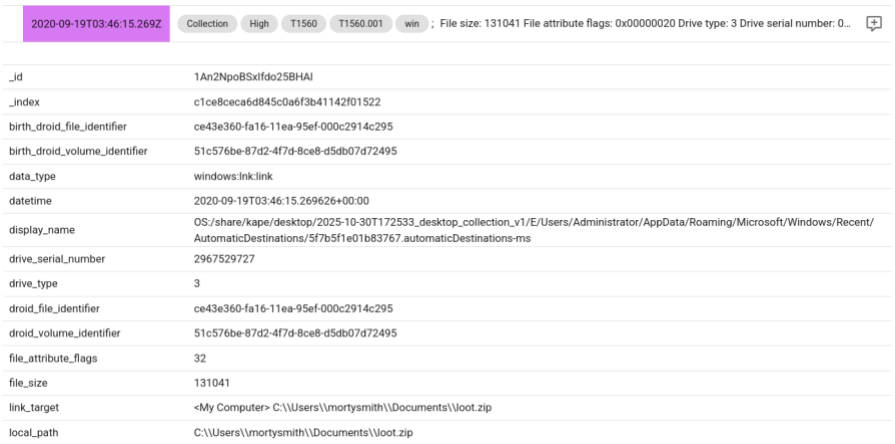


Figure 40. Expanded T1560.001 – Archived Files entry from the desktop triage timeline, showing the creation of the archive loot.zip located at C:\Users\mortysmith\Documents\loot.zip, confirming file compression activity during the incident window.

38. Was Windows Defender disabled on any system? If so, what system (hostname) and was date timestamp? (Hint: Saved Searches > T1562.001-Win Defender Disabled).

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on "T1562.001 – Win Defender Disabled". Then found 2 entries showing when Windows Defender was disabled, as shown in Figure 41.
- **Answer:**
  Windows Defender was disabled on the system, more specifically it was disabled on **DESKTOP-SDN1RPT.C137.local** at **2020-09-19 03:39:45 (247ms) UTC**, as shown in Figure 41.

- **Supporting Evidence:**

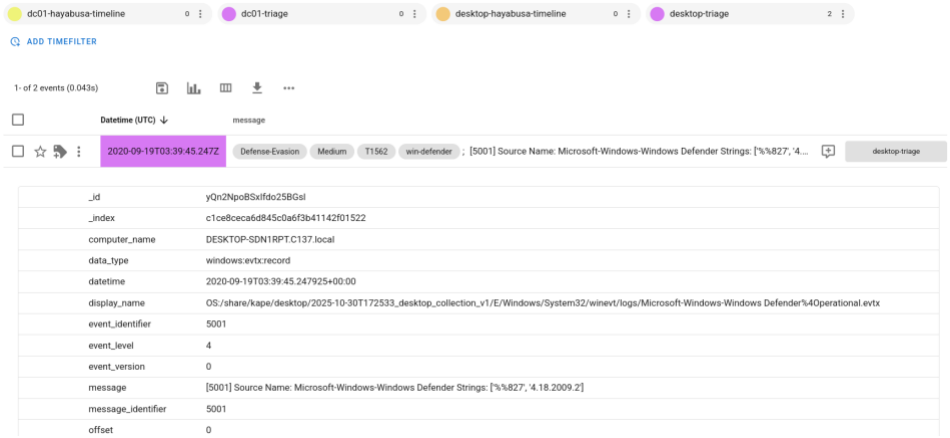


Figure 41. Expanded T1562.001 – Windows Defender Disabled event from the desktop triage timeline, showing that Windows Defender was disabled on DESKTOP-SDN1RPT.C137.local at 2020-09-19 03:39:45 UTC, indicating a defense evasion activity on the compromised system

39. An application crashed on the dc01 system. What is the date timestamp and full path of the application that crashed? (Hint: Saved Searches > Windows Crash activity).

- **Analysis Performed:**
  - In Saved Searches, the examiner clicked on “Windows Crash activity”. Then found 6 entries showing when the application crashed on the dc01 system, as shown in Figure 42.
- **Answer:**
  The date timestamp of the application that crashed is **2020-09-19 03:29:35 (0ms) UTC** and the full path is **C:\Windows\System32\spoolsv.exe**, as shown in Figure 42.

- **Supporting Evidence:**

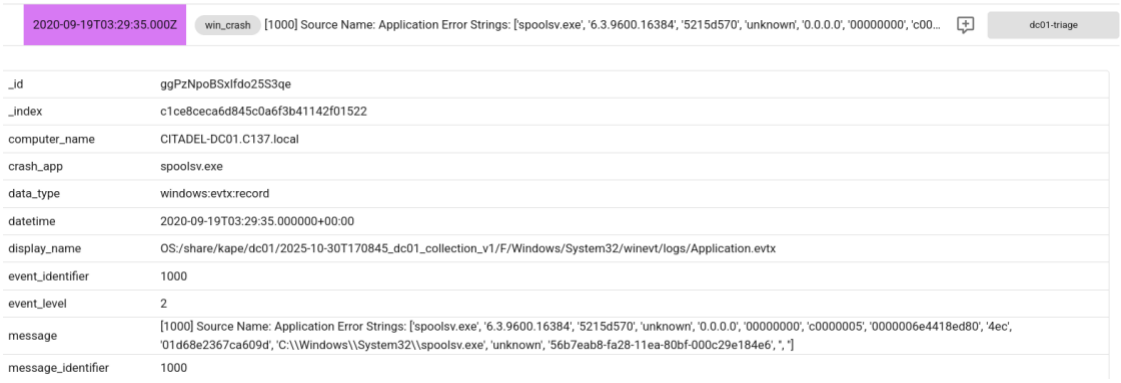
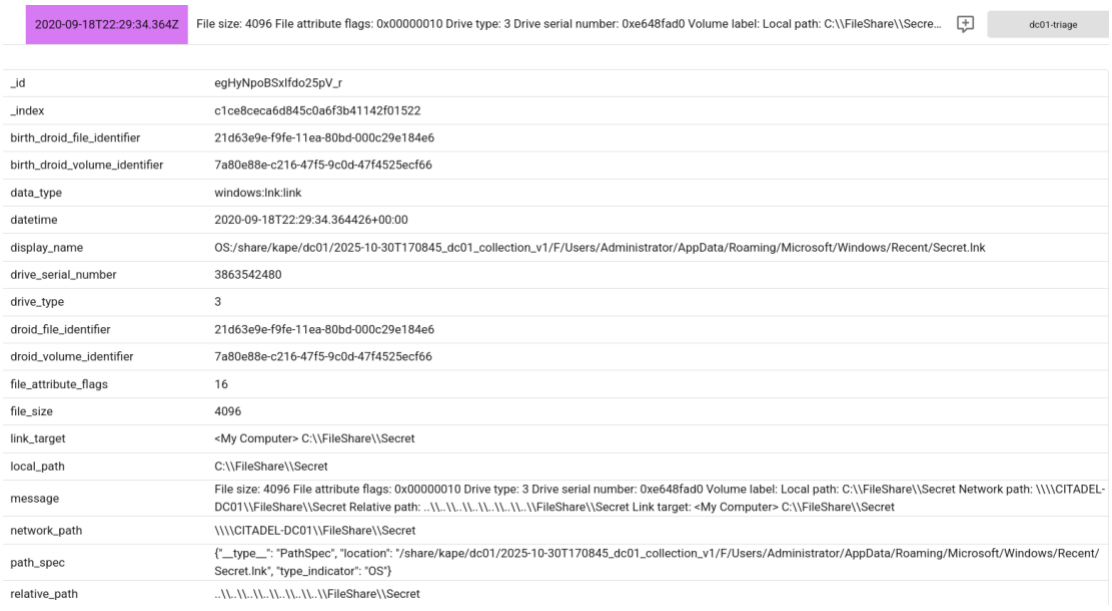


Figure 42. Expanded Windows Crash Activity entry from the dc01 triage timeline, showing that spoolsv.exe crashed on CITADEL-DC01.C137.local at 2020-09-19 03:29:35 UTC, with the executable located at C:\Windows\System32\spoolsv.exe.

40. What is file path of the directory that contains the word "secret"?

- **Analysis Performed:**
  - The examiner searched for the keyword "secret" across all timelines, then searched the first couple of entries and found one where "timestamp_desc" is "Creation Time" and filtered for this value, and additionally filtered for data type: "Windows:lnk:link" to find 12 entries, as shown in Figure 43.
- **Answer:**
  The file path of the directory that contains the word "secret" is **C:\FileShare\Secret**, as shown in Figure 43.

- **Supporting Evidence:**



2020-09-18T22:29:34.364Z	File size: 4096 File attribute flags: 0x00000010 Drive type: 3 Drive serial number: 0xe648fad0 Volume label: Local path: C:\\FileShare\\Secre...	dc01-triage

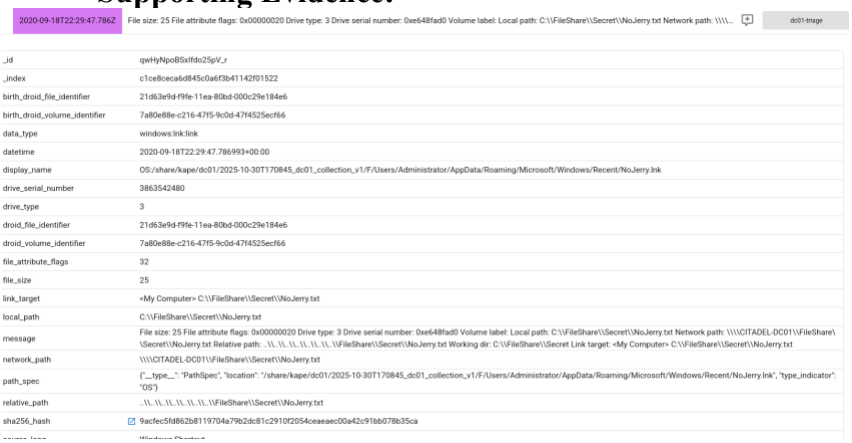
_id	egHyNpoBSxIfdo25pV_r
_index	c1ce8ceca6d845c0a6f3b41142f01522
birth_droid_file_identifier	21d63e9e-f9fe-11ea-80bd-000c29e184e6
birth_droid_volume_identifier	7a80e88e-c216-47f5-9c0d-47f4525ecf66
data_type	windows:lnk:link
datetime	2020-09-18T22:29:34.364426+00:00
display_name	OS:/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/Secret.lnk
drive_serial_number	3863542480
drive_type	3
droid_file_identifier	21d63e9e-f9fe-11ea-80bd-000c29e184e6
droid_volume_identifier	7a80e88e-c216-47f5-9c0d-47f4525ecf66
file_attribute_flags	16
file_size	4096
link_target	<My Computer> C:\\FileShare\\Secret
local_path	C:\\FileShare\\Secret
message	File size: 4096 File attribute flags: 0x00000010 Drive type: 3 Drive serial number: 0xe648fad0 Volume label: Local path: C:\\FileShare\\Secret Network path: \\\\CITADEL-DC01\\FileShare\\Secret Relative path: ..\\..\\..\\..\\..\\..\\..\\FileShare\\Secret Link target: <My Computer> C:\\FileShare\\Secret
network_path	\\\\CITADEL-DC01\\FileShare\\Secret
path_spec	{"__type__": "PathSpec", "location": "/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/Secret.lnk", "type_indicator": "OS"}
relative_path	..\\..\\..\\..\\..\\..\\..\\FileShare\\Secret

Figure 43. Expanded LNK file entry from the dc01 triage timeline, showing a shortcut pointing to the directory C:\FileShare\Secret on CITADEL-DC01, confirming the presence of a folder containing the term "secret."

41. Find the files that have a file size greater than 0 and not 4096. What are the file names?

- **Analysis Performed:**
  - The examiner searched for the keyword “secret” across all timelines, then searched the first couple of entries and found one where “timestamp_desc” is “Creation Time” and filtered for this value, and additionally filtered for data type: “Windows:lnk:link” to find 12 entries.
  - The examiner then filtered for files that have a file size great than 0 and not 4096 which are shown in Figures 44 – 47.
- **Answer:**
  The filename of the file that has a file size of 25 is **NoJerry.txt**, as shown in Figure 44. The filename of the file that has a file size of 143 is **PortalGunPlans.txt**, as shown in Figure 45. The filename of the file that has a file size of 478 is **Szechuan Sauce.txt**, as shown in Figure 46. The filename of the file that has a file size of 28 is **SECRET_beth.txt**, as shown in Figure 47.

- **Supporting Evidence:**



2020-09-18T22:29:47.786Z	File size: 25 File attribute flags: 0x00000020 Drive type: 3 Drive serial number: 0xe648fad0 Volume label: Local path: C:\\FileShare\\Secret\\NoJerry.txt Network path: \\\\... dc01-triage
_id	qwHyNpoBSxIfdo25pV_r
_index	c1ce8ceca6d845c0a6f3b41142f01522
birth_droid_file_identifier	21d63e9d-f9fe-11ea-80bd-000c29e184e6
birth_droid_volume_identifier	7a80e88e-c216-47f5-9c0d-47f4525ecf66
data_type	windows:lnk:link
datetime	2020-09-18T22:29:47.786993+00:00
display_name	OS:/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/NoJerry.lnk
drive_serial_number	3863542480
drive_type	3
droid_file_identifier	21d63e9d-f9fe-11ea-80bd-000c29e184e6
droid_volume_identifier	7a80e88e-c216-47f5-9c0d-47f4525ecf66
file_attribute_flags	32
file_size	25
link_target	<My Computer> C:\\FileShare\\Secret\\NoJerry.txt
local_path	C:\\FileShare\\Secret\\NoJerry.txt
message	File size: 25 File attribute flags: 0x00000020 Drive type: 3 Drive serial number: 0xe648fad0 Volume label: Local path: C:\\FileShare\\Secret\\NoJerry.txt Network path: \\\\CITADEL-DC01\\FileShare\\Secret\\NoJerry.txt Relative path: ..\\..\\..\\..\\..\\..\\..\\..\\FileShare\\Secret\\NoJerry.txt Working dir: C:\\FileShare\\Secret Link target: <My Computer> C:\\FileShare\\Secret\\NoJerry.txt
network_path	\\\\CITADEL-DC01\\FileShare\\Secret\\NoJerry.txt
path_spec	{"__type__": "PathSpec", "location": "/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/NoJerry.lnk", "type_indicator": "OS"}
relative_path	..\\..\\..\\..\\..\\..\\..\\..\\FileShare\\Secret\\NoJerry.txt
sha256_hash	9acfec5fd862b8119704a79b2dc81c2910f2054ceaeaec00a42c91bb078b35ca

Figure 44. Expanded LNK file entry from the dc01 triage timeline, showing a shortcut to NoJerry.txt located in C:\FileShare\Secret\, with a file size of 25 bytes, indicating a small text file rather than a standard 4096-byte link placeholder.

2020-09-18T22:33:54.432Z	File size: 143 File attribute flags: 0x00000020 Drive type: 3 Drive serial number: 0xe648fad0 Volume label: Local path: C:\\FileShare\\Secret\\PortalGunPlans.txt Network ... dc01-triage
_id	RwHyNpoBSxIfdo25pWLr
_index	c1ce8ceca6d845c0a6f3b41142f01522
birth_droid_file_identifier	21d63eda-f9fe-11ea-80bd-000c29e184e6
birth_droid_volume_identifier	7a80e88e-c216-47f5-9c0d-47f4525ecf66
data_type	windows:lnk:link
datetime	2020-09-18T22:33:54.432582+00:00
display_name	OS:/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/PortalGunPlans.lnk
drive_serial_number	3863542480
drive_type	3
droid_file_identifier	21d63eda-f9fe-11ea-80bd-000c29e184e6
droid_volume_identifier	7a80e88e-c216-47f5-9c0d-47f4525ecf66
file_attribute_flags	32
file_size	143
link_target	<My Computer> C:\\FileShare\\Secret\\PortalGunPlans.txt
local_path	C:\\FileShare\\Secret\\PortalGunPlans.txt
message	File size: 143 File attribute flags: 0x00000020 Drive type: 3 Drive serial number: 0xe648fad0 Volume label: Local path: C:\\FileShare\\Secret\\PortalGunPlans.txt Network path: \\\\CITADEL-DC01\\FileShare\\Secret\\PortalGunPlans.txt Relative path: ..\\..\\..\\..\\..\\..\\..\\..\\FileShare\\Secret\\PortalGunPlans.txt Working dir: C:\\FileShare\\Secret Link target: <My Computer> C:\\FileShare\\Secret\\PortalGunPlans.txt
network_path	\\\\CITADEL-DC01\\FileShare\\Secret\\PortalGunPlans.txt
path_spec	{"__type__": "PathSpec", "location": "/share/kape/dc01/2025-10-30T170845_dc01_collection_v1/F/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/PortalGunPlans.lnk", "type_indicator": "OS"}
relative_path	..\\..\\..\\..\\..\\..\\..\\..\\FileShare\\Secret\\PortalGunPlans.txt
sha256_hash	c03520c5f580f2da581475051e28551d8975f912a894324898cc5143b7db6b6c

Figure 45. Expanded LNK file entry from the dc01 triage timeline, showing a shortcut to PortalGunPlans.txt stored in C:\FileShare\Secret\, with a file size of 143 bytes, marking it as one of the small files found in the secret directory.

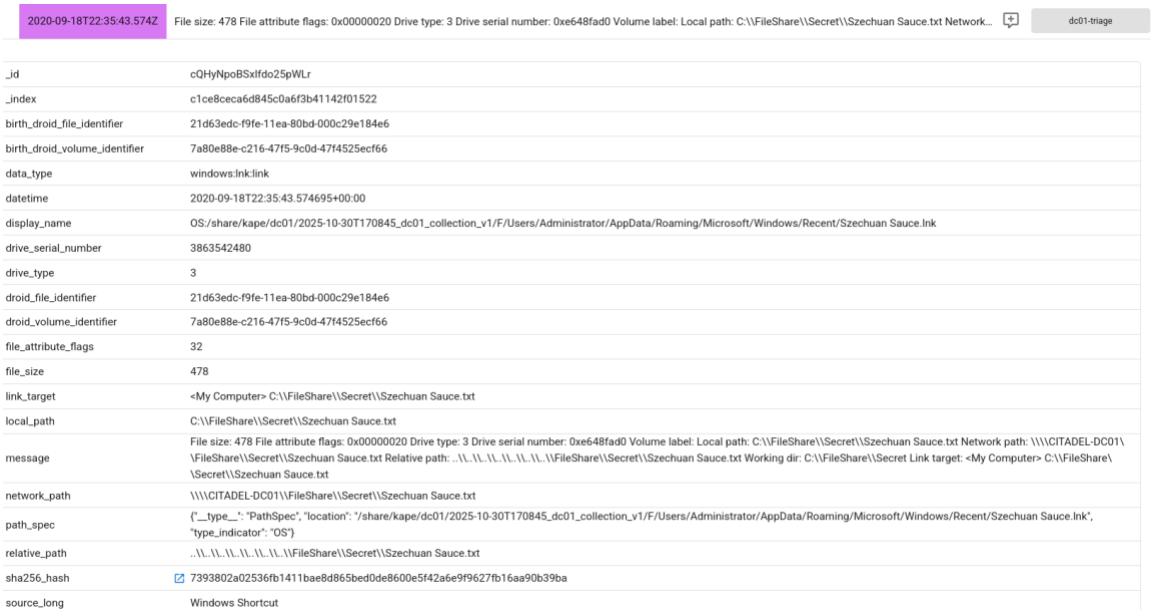


Figure 46. Expanded LNK file entry from the dc01 triage timeline, showing a shortcut to Szechuan Sauce.txt located in C:\FileShare\Secret\, with a file size of 478 bytes, identifying it as another small text file within the secret directory.

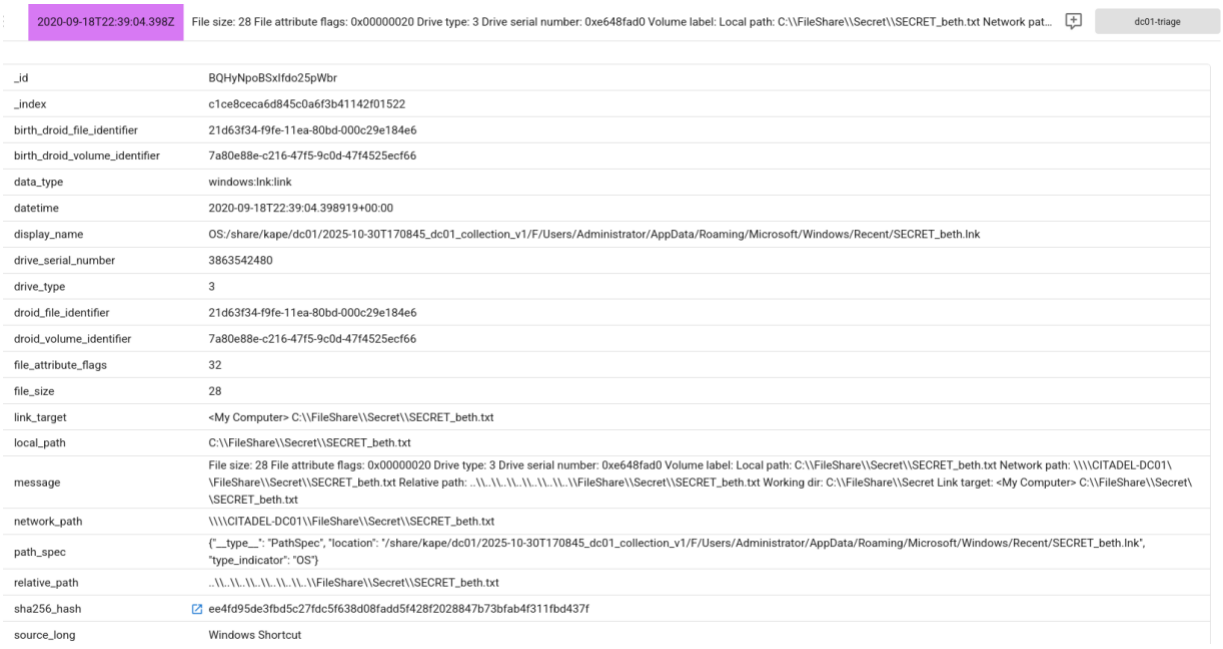


Figure 47. Expanded LNK file entry from the dc01 triage timeline, showing a shortcut to SECRET_beth.txt in C:\FileShare\Secret\, with a file size of 28 bytes, indicating a small text document associated with the secret directory contents.

Conclusion

The examiner, Inor Wang, enjoyed this lab. There is no critique from me. Thank you.

References

Carvey, H. A. (2014). Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8 (Fourth edition). Syngress.

Johansen, G., & Safari, an O. M. C. (2020). Digital Forensics and Incident Response—Second Edition.

Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory. Wiley.

Malware forensics field guide for Windows systems digital forensics field guides. (2012). Syngress.

Oettinger, W., & Safari, an O. M. C. (2020). Learn Computer Forensics.

Reddy, N. (2019). Practical cyber forensics: An incident-based approach to forensic investigations. APress. https://doi.org/10.1007/978-1-4842-4460-9.