Auditing Midterm – Practical

Jackson Yuan

Faculty of Applied Science & Technology, Sheridan College Institute of Technology and Advanced Learning

INFO30004: Information Systems Security Auditing

Pedram Habibi

March 3, 2023

Table of Contents

Part 1 – Phantom Playbook

For this phantom playbook, I will try to investigate a suspicious email artifact that I created on a custom playbook. First step is I created a new suspicious email container with 2 suspicious artifacts which are of email type and with the IP address of those emails as shown in Figure 13. Now we run it in the phantom playbook by adding: **phantom.debug(container)** in which we can clearly see the number of artifacts created (which is 2) and the description of our event name container in Figure 14 and Figure 14.1. Now, the next step is we want to print out all the artifact's IP address within our container. To do so, we must invoke the collect() function in phantom as this will "gather information from the associated artifacts of a container" [6]. As a result, we do this by adding the code along with the associated parameters as shown in Figure 15 [6]. As a result, we save and run it on the new container created as aforementioned and the results are as expected which are the correct IP addresses of the suspicious emails as shown in Figure 16 and Figure 16.1. Finally, we check the debugger log to verify and confirm that the files were actually ran and what was displayed on screen in Figure 16 was legitimate, this is hold true as shown in Figure 17.

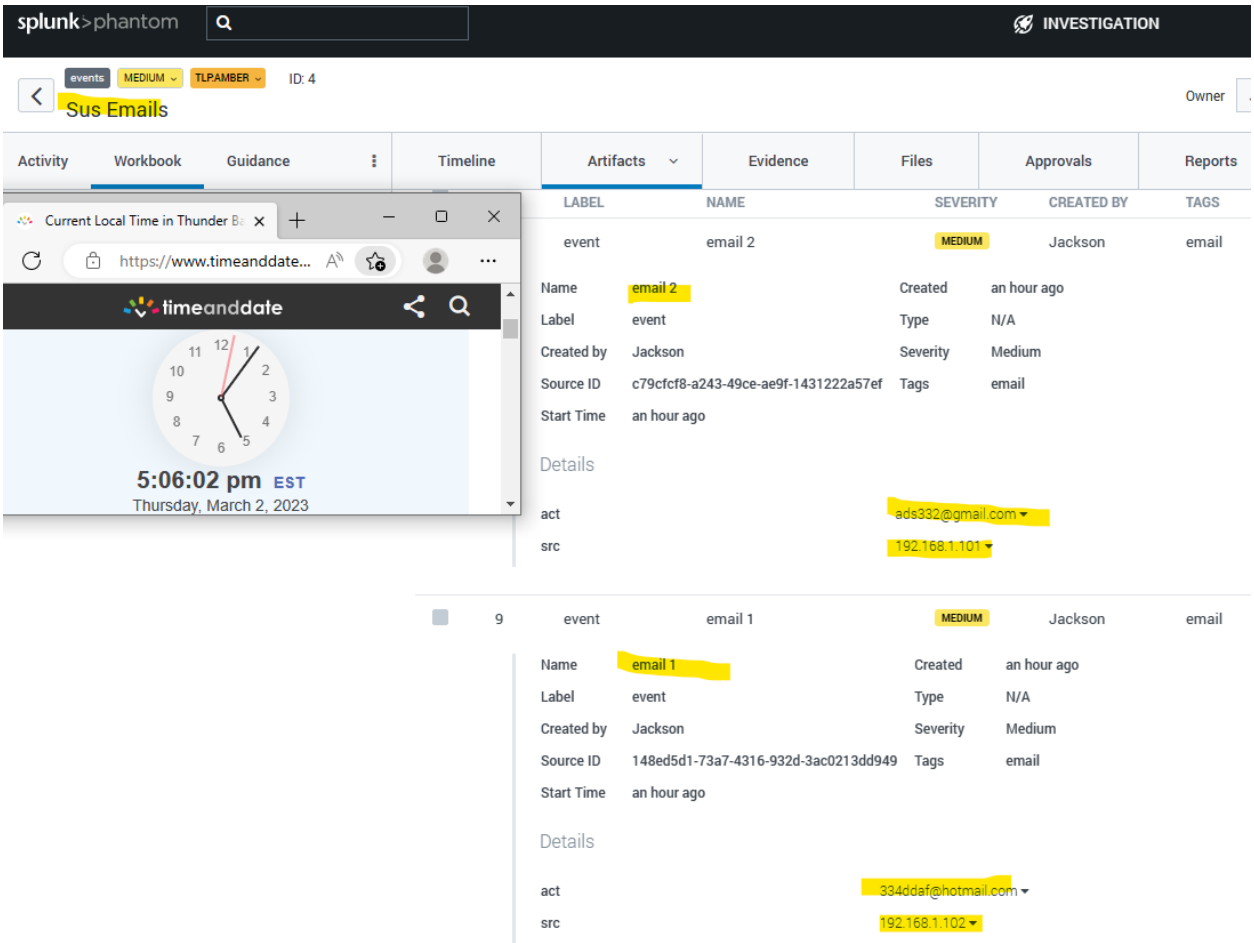


Figure 13 ↑

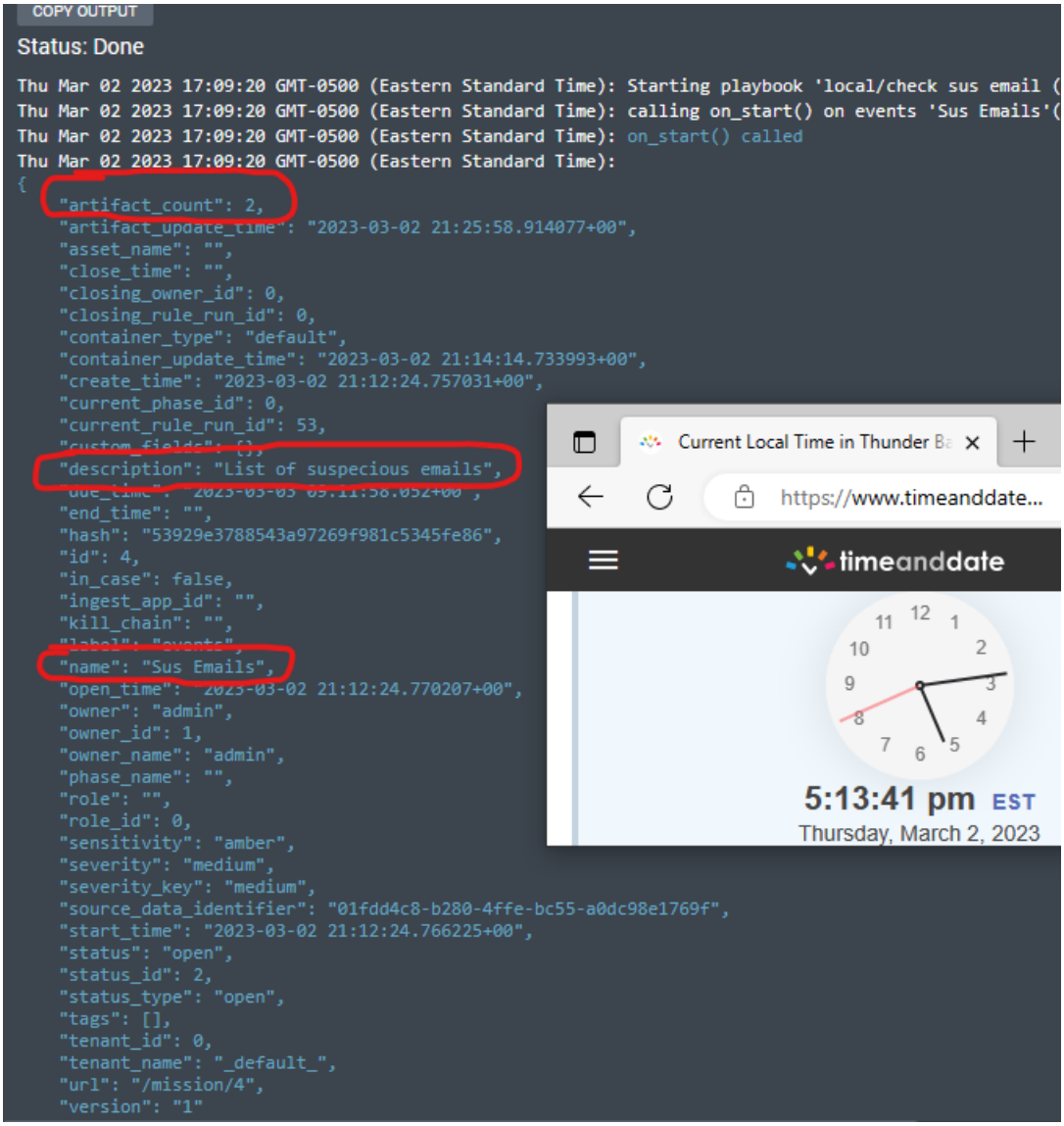

COPY OUTPUT
Status: Done
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): Starting playbook 'local/check sus email (
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): calling on_start() on events 'Sus Emails'(
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): on_start() called
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time):
{
"artifact_count": 2,
"artifact_update_time": "2023-03-02 21:25:58.914077+00",
"asset_name": "",
"close_time": "",
"closing_owner_id": 0,
"closing_rule_run_id": 0,
"container_type": "default",
"container_update_time": "2023-03-02 21:14:14.733993+00",
"create_time": "2023-03-02 21:12:24.757031+00",
"current_phase_id": 0,
"current_rule_run_id": 53,
"description": "List of suspecious emails",
"end_time": "",
"hash": "53929e3788543a97269f981c5345fe86",
"id": 4,
"in_case": false,
"ingest_app_id": "",
"kill_chain": "",
"name": "Sus Emails",
"open_time": "2023-03-02 21:12:24.770207+00",
"owner": "admin",
"owner_id": 1,
"owner_name": "admin",
"phase_name": "",
"role": "",
"role_id": 0,
"sensitivity": "amber",
"severity": "medium",
"severity_key": "medium",
"source_data_identifier": "01fdd4c8-b280-4ffe-bc55-a0dc98e1769f",
"start_time": "2023-03-02 21:12:24.766225+00",
"status": "open",
"status_id": 2,
"status_type": "open",
"tags": [],
"tenant_id": 0,
"tenant_name": "_default_",
"url": "/mission/4",
"version": "1"
Current Local Time in Thunder B
https://www.timeanddate...
timeanddate
5:13:41 pm EST
Thursday, March 2, 2023

Figure 14 ↑

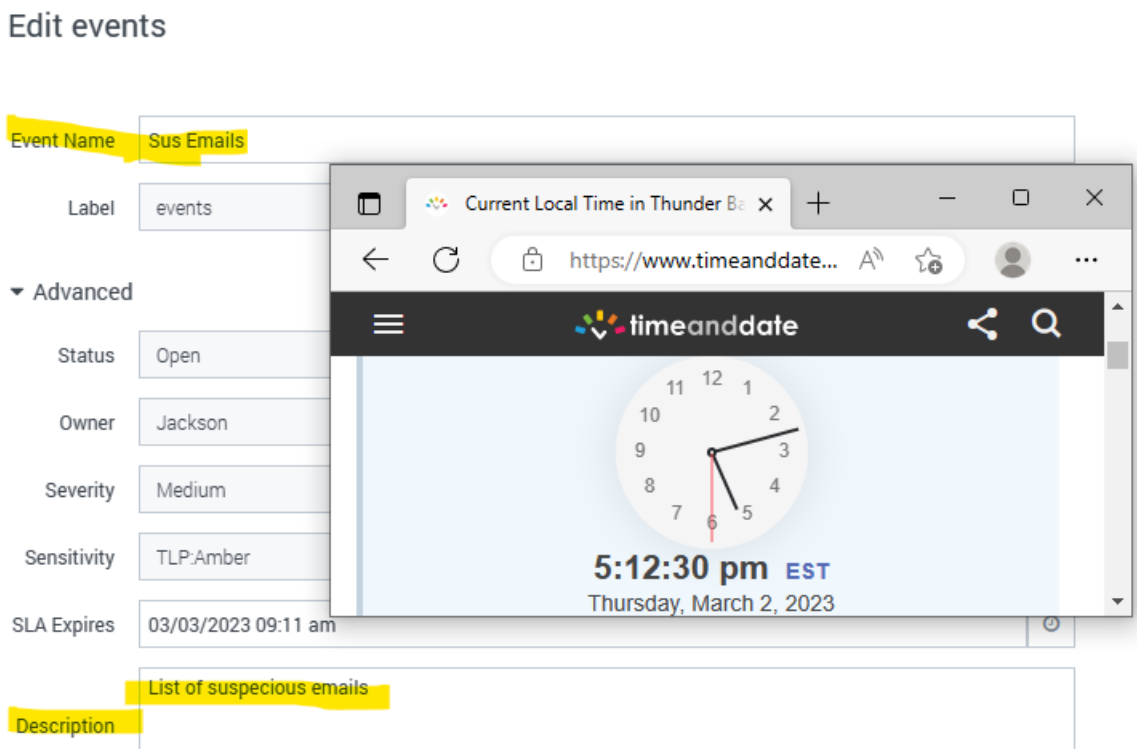


Figure 14.1↑

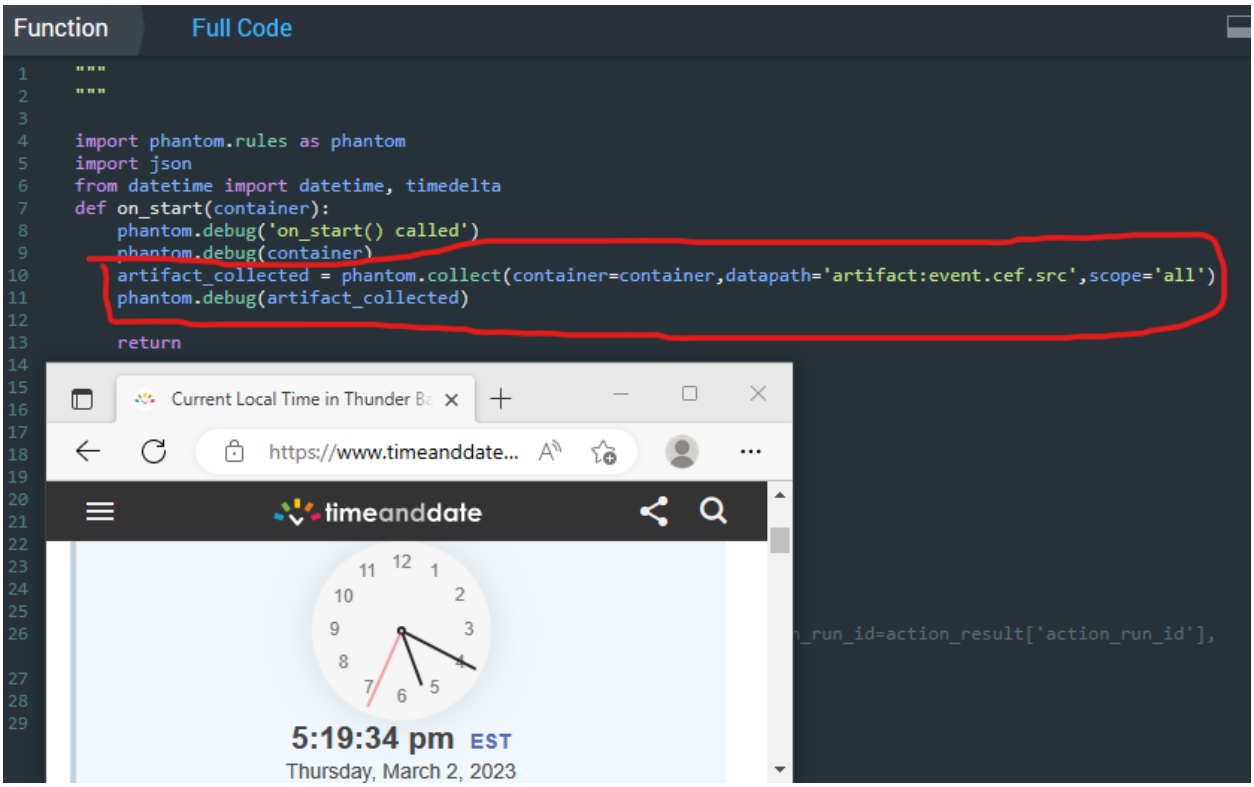


Figure 15↑

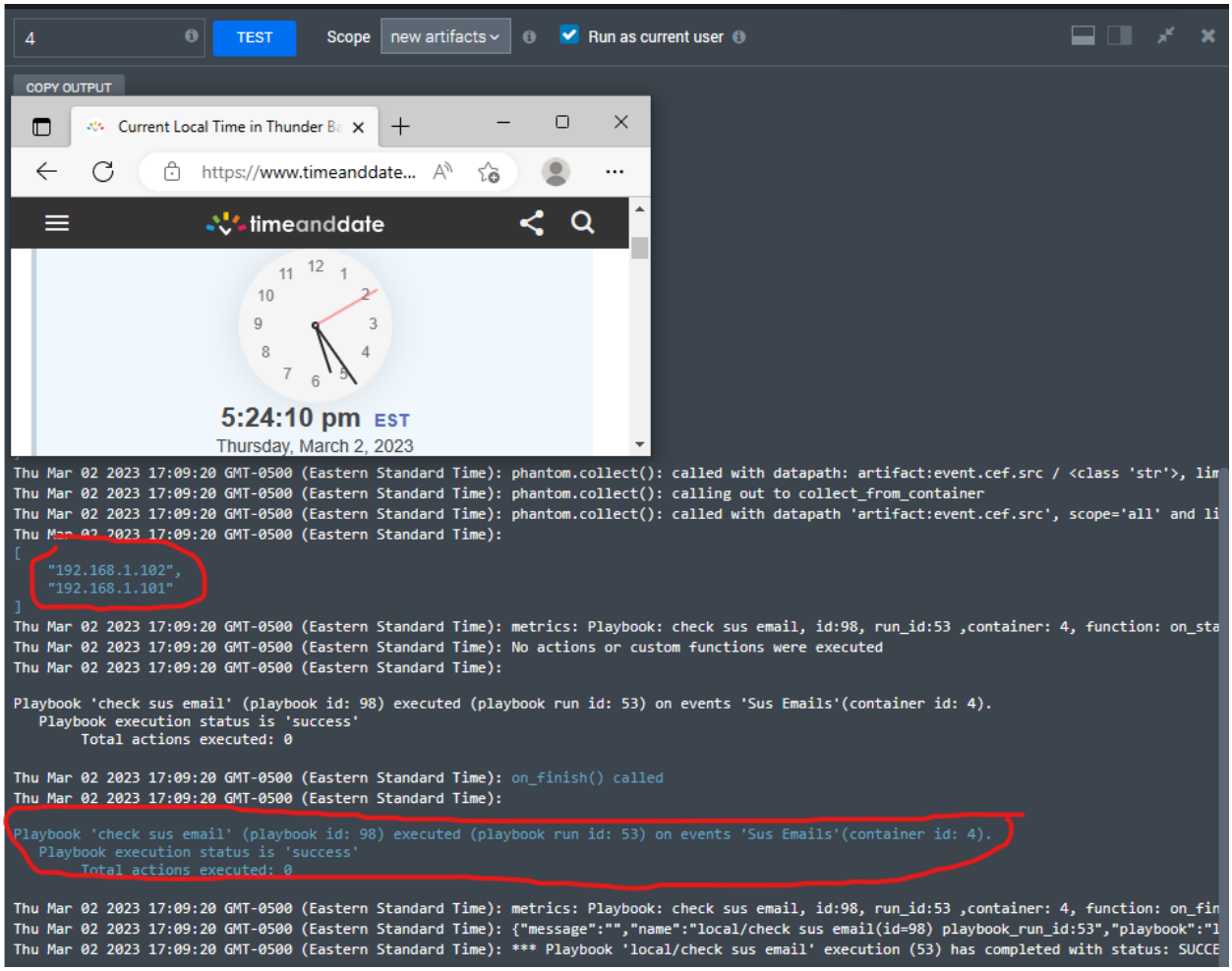

4
TEST
Scope
new artifacts
Run as current user
COPY OUTPUT
Current Local Time in Thunder Ba
https://www.timeanddate...
timeanddate
5:24:10 pm EST
Thursday, March 2, 2023
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): phantom.collect(): called with datapath: artifact:event.cef.src / <class 'str'>, lim
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): phantom.collect(): calling out to collect_from_container
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): phantom.collect(): called with datapath 'artifact:event.cef.src', scope='all' and li
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time):
[
"192.168.1.102",
"192.168.1.101"
]
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): metrics: Playbook: check sus email, id:98, run_id:53 ,container: 4, function: on_sta
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): No actions or custom functions were executed
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time):
Playbook 'check sus email' (playbook id: 98) executed (playbook run id: 53) on events 'Sus Emails'(container id: 4).
Playbook execution status is 'success'
Total actions executed: 0
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): on_finish() called
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time):
Playbook 'check sus email' (playbook id: 98) executed (playbook run id: 53) on events 'Sus Emails'(container id: 4).
Playbook execution status is 'success'
Total actions executed: 0
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): metrics: Playbook: check sus email, id:98, run_id:53 ,container: 4, function: on_fin
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): {"message":"","name":"local/check sus email(id=98) playbook_run_id:53","playbook":"1
Thu Mar 02 2023 17:09:20 GMT-0500 (Eastern Standard Time): *** Playbook 'local/check sus email' execution (53) has completed with status: SUCCE

Figure 16↑

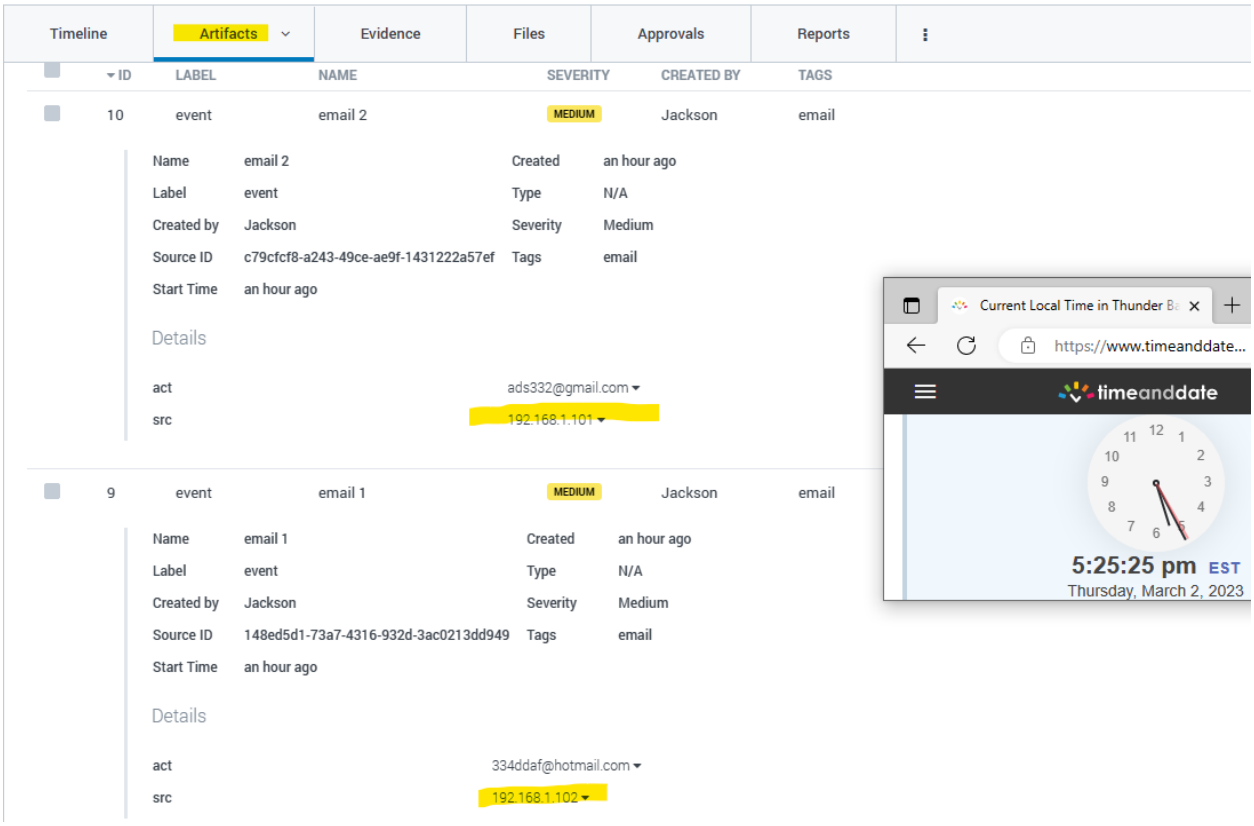

Timeline
Artifacts
Evidence
Files
Approvals
Reports
ID
LABEL
NAME
SEVERITY
CREATED BY
TAGS
10
event
email 2
MEDIUM
Jackson
email
Name
email 2
Created
an hour ago
Label
event
Type
N/A
Created by
Jackson
Severity
Medium
Source ID
c79cfcf8-a243-49ce-ae9f-1431222a57ef
Tags
email
Start Time
an hour ago
Details
act
ads332@gmail.com
src
192.168.1.101
9
event
email 1
MEDIUM
Jackson
email
Name
email 1
Created
an hour ago
Label
event
Type
N/A
Created by
Jackson
Severity
Medium
Source ID
148ed5d1-73a7-4316-932d-3ac0213dd949
Tags
email
Start Time
an hour ago
Details
act
334ddaf@hotmail.com
src
192.168.1.102
Current Local Time in Thunder B
https://www.timeanddate...
timeanddate
5:25:25 pm EST
Thursday, March 2, 2023

Figure 16.1↑

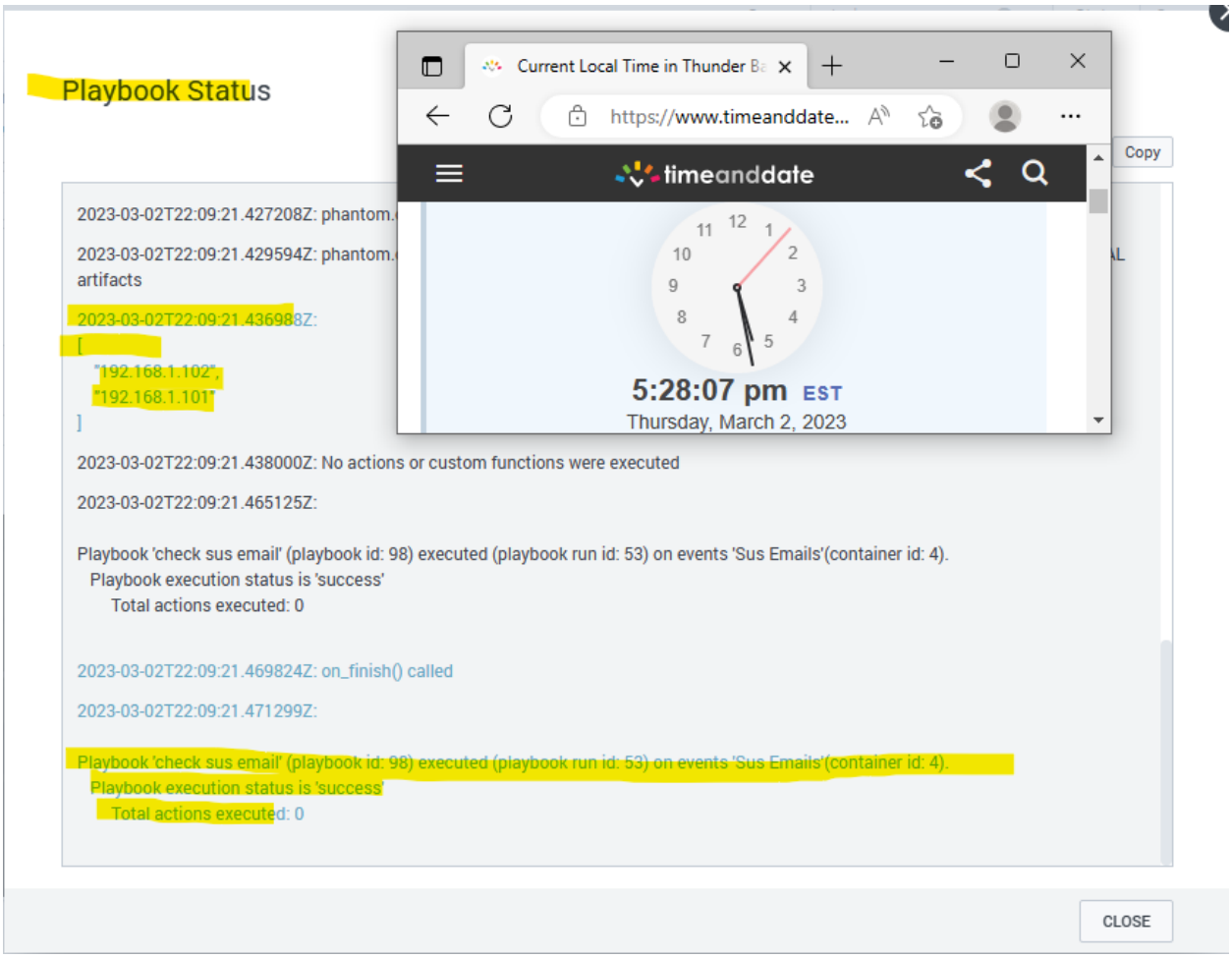

Playbook Status
Copy
2023-03-02T22:09:21.427208Z: phantom.
2023-03-02T22:09:21.429594Z: phantom.
artifacts
2023-03-02T22:09:21.436988Z:
[
"192.168.1.102",
"192.168.1.101"
]
2023-03-02T22:09:21.438000Z: No actions or custom functions were executed
2023-03-02T22:09:21.465125Z:
Playbook 'check sus email' (playbook id: 98) executed (playbook run id: 53) on events 'Sus Emails'(container id: 4).
Playbook execution status is 'success'
Total actions executed: 0
2023-03-02T22:09:21.469824Z: on_finish() called
2023-03-02T22:09:21.471299Z:
Playbook 'check sus email' (playbook id: 98) executed (playbook run id: 53) on events 'Sus Emails'(container id: 4).
Playbook execution status is 'success'
Total actions executed: 0
CLOSE
Current Local Time in Thunder Ba
https://www.timeanddate...
timeanddate
5:28:07 pm EST
Thursday, March 2, 2023

Figure 17↑

Part 2 – Incident Response

Question #1

The attacker pivoted to another workstation using credentials gained from Minty's computer. Which account name was used to pivot to another machine?

Answer

To search for the account name, we must first understand who the attacker is and when he was able to successfully login as he "pivoted to another machine". Using the answer found in the demo shown by professor Habibi [1], we can see that the attackers IP address is "192.168.247.175" as shown in Figure 1. Second, we must understand what happens when a user logs on and this must have been kept tracked in windows event logger. By definition, when an account is successfully logged on, windows event log generates an ID of 4624 [2]. The final search query will be this: **source="Minty_download_malicious_activity.csv" host="localhost.localdomain" index="main" sourcetype="csv" SourceNetworkAddress="192.168.247.175" EventID="4624"** shown in Figure 2 and upon searching through the strings we find an account named "alabaster". To verify if this holds for all the cases, we build a table with the command: **source="Minty_download_malicious_activity.csv" host="localhost.localdomain" index="main" sourcetype="csv" |table EventID SourceNetworkAddress AccountName |where SourceNetworkAddress="192.168.247.175" AND EventID="4624"** as shown in Figure 3 below and it shows that the only person to successfully login with that specific IP is "alabaster".

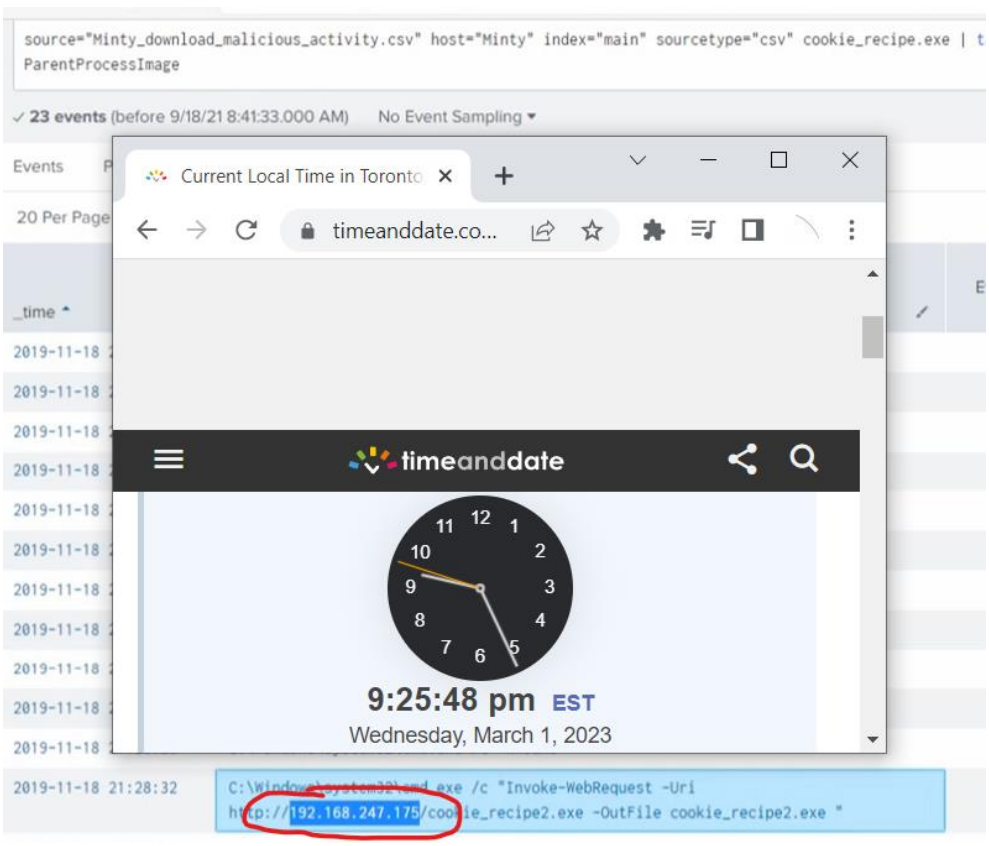


Figure 1 ↑

Source: [1]

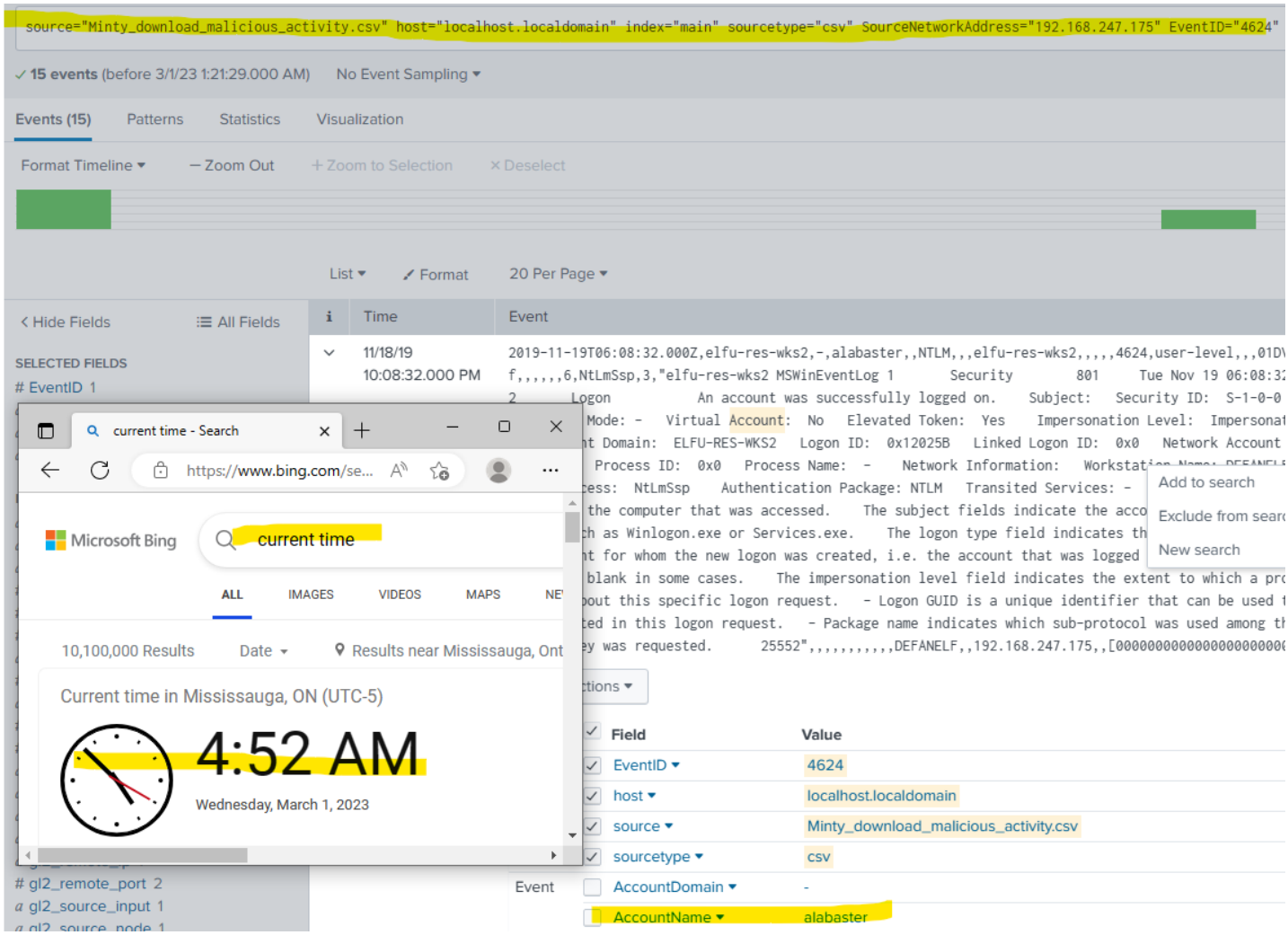

source="Minty_download_malicious_activity.csv" host="localhost.localdomain" index="main" sourcetype="csv" SourceNetworkAddress="192.168.247.175" EventID="4624"
15 events (before 3/1/23 1:21:29.000 AM)
No Event Sampling
Events (15)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
EventID 1
Time
Event
11/18/19
10:08:32.000 PM
current time - Search
https://www.bing.com/se...
Microsoft Bing
current time
ALL
IMAGES
VIDEOS
MAPS
10,100,000 Results
Date
Results near Mississauga, Ont
Current time in Mississauga, ON (UTC-5)
4:52 AM
Wednesday, March 1, 2023
Add to search
Exclude from searc
New search
Field
Value
EventID
4624
host
localhost.localdomain
source
Minty_download_malicious_activity.csv
sourcetype
csv
Event
AccountDomain
-
AccountName
alabaster
gl2_remote_port 2
a gl2_source_input 1

Figure 2 ↑

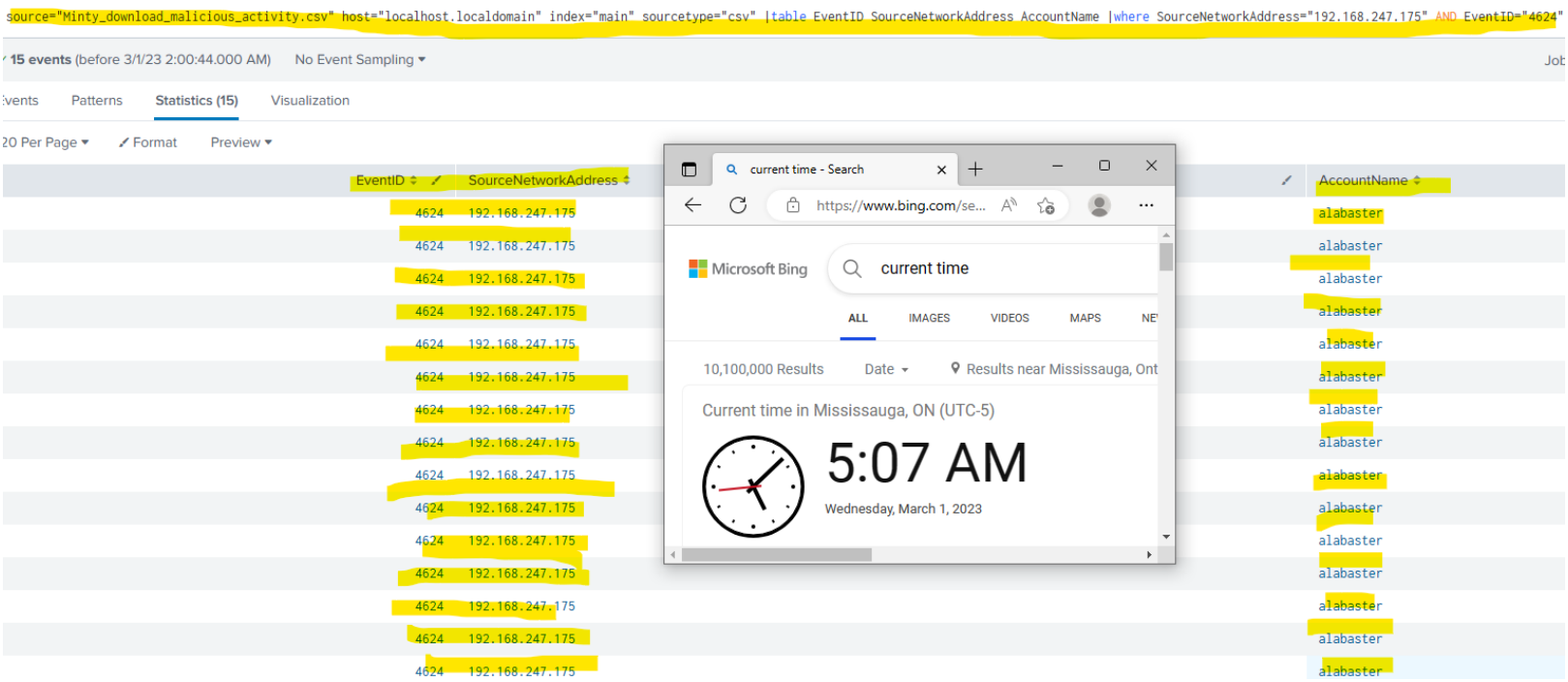

source="Minty_download_malicious_activity.csv" host="localhost.localdomain" index="main" sourcetype="csv" |table EventID SourceNetworkAddress AccountName |where SourceNetworkAddress="192.168.247.175" AND EventID="4624"
15 events (before 3/1/23 2:00:44.000 AM)
No Event Sampling
Patterns
Statistics (15)
Visualization
20 Per Page
Format
Preview
EventID
SourceNetworkAddress
AccountName
4624 192.168.247.175 alabaster
current time - Search
https://www.bing.com/se...
Microsoft Bing
current time
ALL
IMAGES
VIDEOS
MAPS
10,100,000 Results
Date
Results near Mississauga, Ont
Current time in Mississauga, ON (UTC-5)
5:07 AM
Wednesday, March 1, 2023

Figure 3 ↑

Question #2

What is the time (HH: MM: SS) the attacker makes a Remote Desktop connection to another machine?

Answer

According to [2], a Remote Desktop login would be defined as having the Logon Type as 10 which states "RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)" [2]. Hence, the search query will be the following: **source="Minty_download_malicious_activity.csv" host="localhost.localdomain" index="main" sourcetype="csv" SourceNetworkAddress="192.168.247.175" EventID="4624" LogonType="10"**. This gives us the time of "**06:04:28**" as shown below in Figure 4.

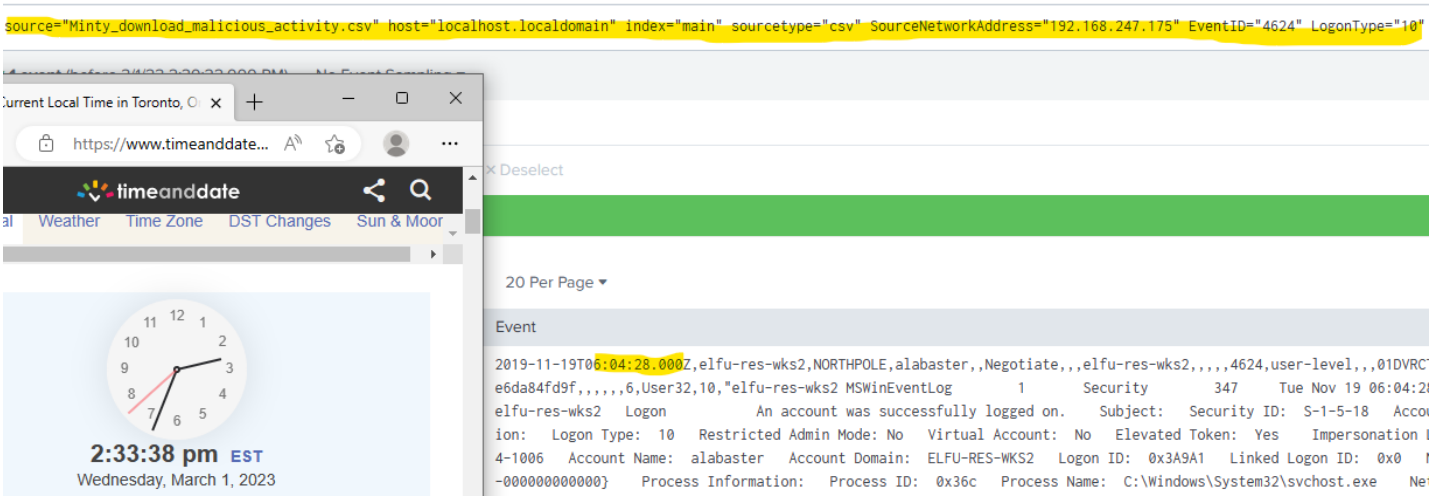


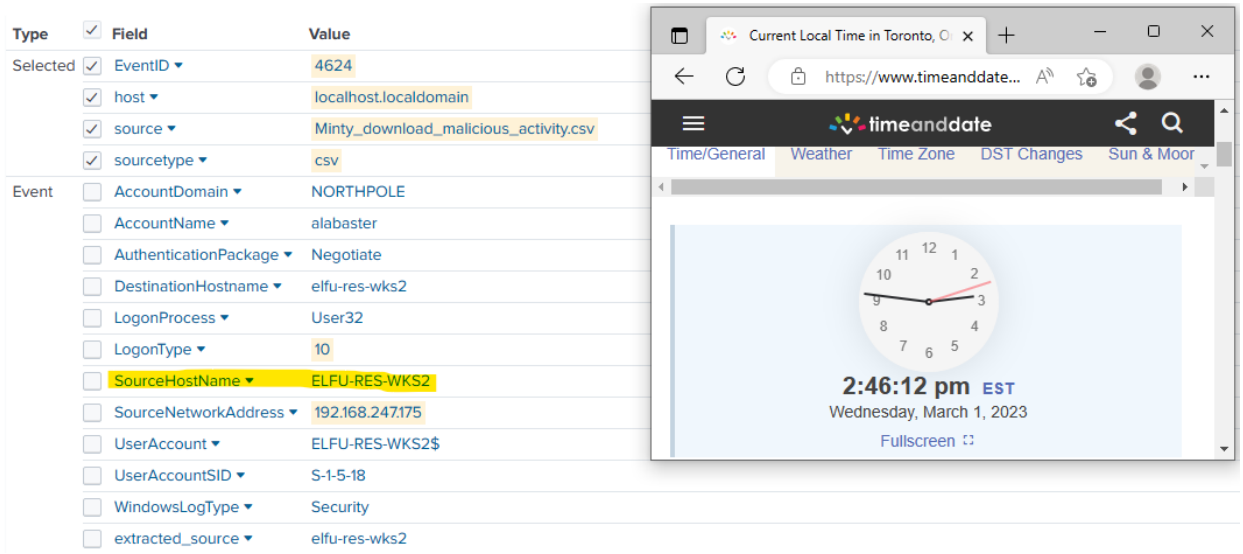
Figure 4 ↑

Question #3

The attacker navigates the file system of a third host using their Remote Desktop Connection to the second host. What is the SourceHostName, DestinationHostname, LogonType of this connection?

Answer

Armed with our previous knowledge, we noticed that the source host name is also listed as shown in Figure 5. This must be the attackers source host name thus we can use this in our search. Hence, our following query will be like this: **source="Minty_download_malicious_activity.csv" host="localhost.localdomain" index="main" sourcetype="csv" SourceHostName="ELFU-RES-WKS2" EventID="4624"**. A LogonType=3 is correct as the attacker has navigated the filesystem to connect to a third host through RDP which by definition is a "connection to shared folder on this computer from elsewhere on network" [2]. Hence, the SourceHostName = **ELFU-RES-WKS2**, DestinationHostname = **elfu-res-wks3**, and LogonType=**3** as shown in Figure 6.



Type	Field	Value
Selected	EventID	4624
	host	localhost.localdomain
	source	Minty_download_malicious_activity.csv
	sourcetype	csv
Event	AccountDomain	NORTHPOLE
	AccountName	alabaster
	AuthenticationPackage	Negotiate
	DestinationHostname	elfu-res-wks2
	LogonProcess	User32
	LogonType	10
	SourceHostName	ELFU-RES-WKS2
	SourceNetworkAddress	192.168.247.175
	UserAccount	ELFU-RES-WKS2$
	UserAccountSID	S-1-5-18
	WindowsLogType	Security
	extracted_source	elfu-res-wks2

Figure 5 ↑

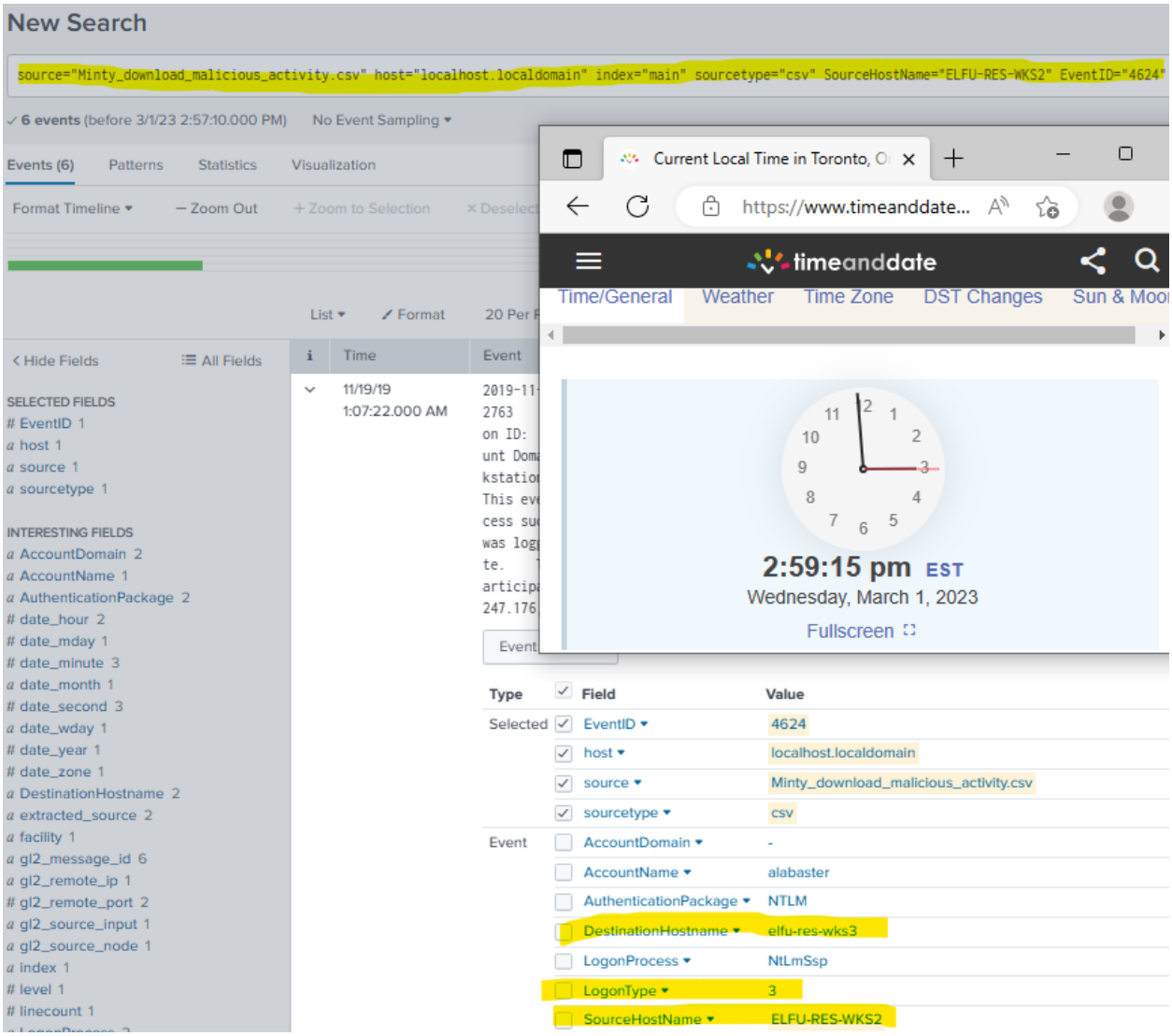

New Search
source="Minty_download_malicious_activity.csv" host="localhost.localdomain" index="main" sourcetype="csv" SourceHostName="ELFU-RES-WKS2" EventID="4624"
6 events (before 3/1/23 2:57:10.000 PM)
No Event Sampling
Events (6)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Current Local Time in Toronto, O
https://www.timeanddate...
timeanddate
Time/General
Weather
Time Zone
DST Changes
Sun & Moo
List
Format
Hide Fields
All Fields
Time
Event
11/19/19 1:07:22.000 AM
SELECTED FIELDS
EventID 1
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a AccountDomain 2
a AccountName 1
a AuthenticationPackage 2
date_hour 2
date_mday 1
date_minute 3
a date_month 1
date_second 3
a date_wday 1
date_year 1
date_zone 1
a DestinationHostname 2
a extracted_source 2
a facility 1
a gl2_message_id 6
a gl2_remote_ip 1
gl2_remote_port 2
a gl2_source_input 1
a gl2_source_node 1
a index 1
level 1
linecount 1
2:59:15 pm EST
Wednesday, March 1, 2023
Fullscreen
Type
Field
Value
Selected
EventID
4624
host
localhost.localdomain
source
Minty_download_malicious_activity.csv
sourcetype
csv
Event
AccountDomain
-
AccountName
alabaster
AuthenticationPackage
NTLM
DestinationHostname
elfu-res-wks3
LogonProcess
NtLmSsp
LogonType
3
SourceHostName
ELFU-RES-WKS2

Figure 6 ↑

Question #4

What is the full-path + filename of the secret research document after being transferred from the third host to the second host?

Answer

From our previous question, our second host is defined as “elfu-res-wks2” and by definition, a Window’s (aka Sysmon) Event ID of 2 is “a process changed a file creation time” which is what happens when you transfer a file from one location to another [3]. Once we search that, we have narrowed our window down to 78 searches as shown in Figure 7. To further refine the search, we use the “search” key word and define the query as all valid popular extensions [4]. This narrows it down to 9 search results as shown in figure 8. The results give us only two options, .txt and .pdf extensions. However, upon further inspection all .txt file extensions are either system log files or just temporary app data being stored by the computer. Hence, by using the process of elimination we can conclude that the .pdf must be the file that was transferred. Moreover, the name itself also alludes to the fact that it’s a “secret” document as shown in Figure 8.1. So, the full file path is:
C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf and the filename is:
super_secret_elfu_research.pdf.

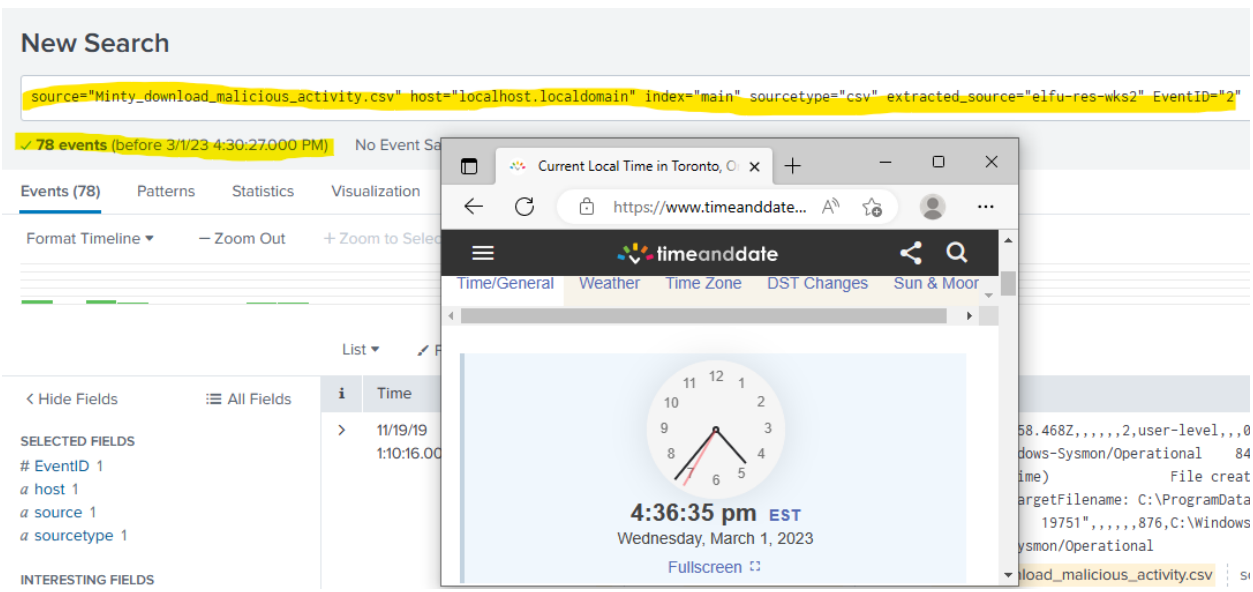


Figure 7 ↑

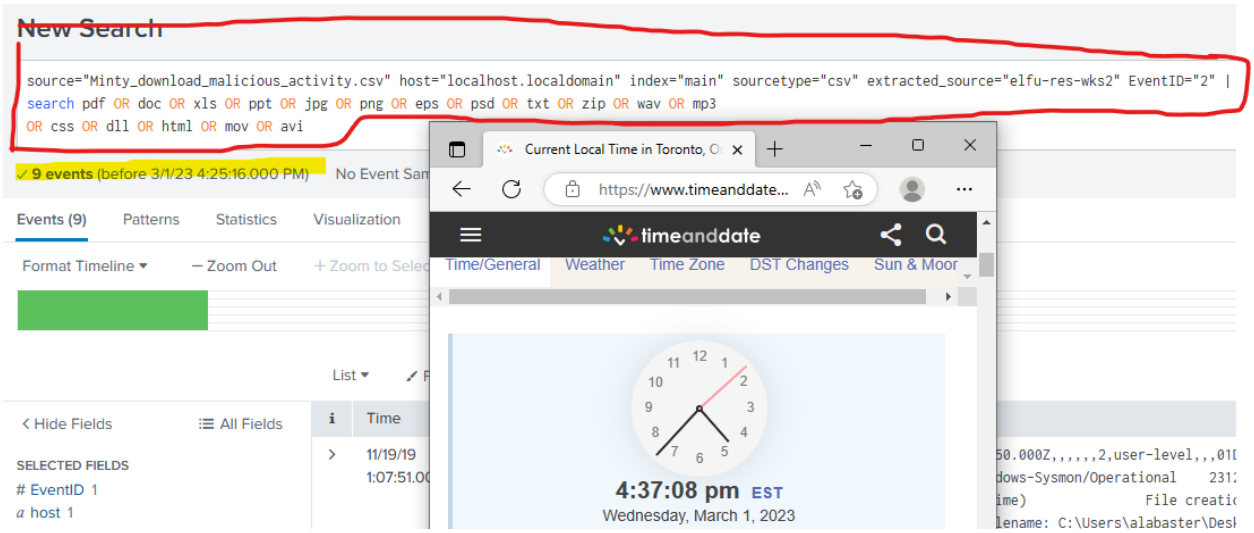


Figure 8 ↑

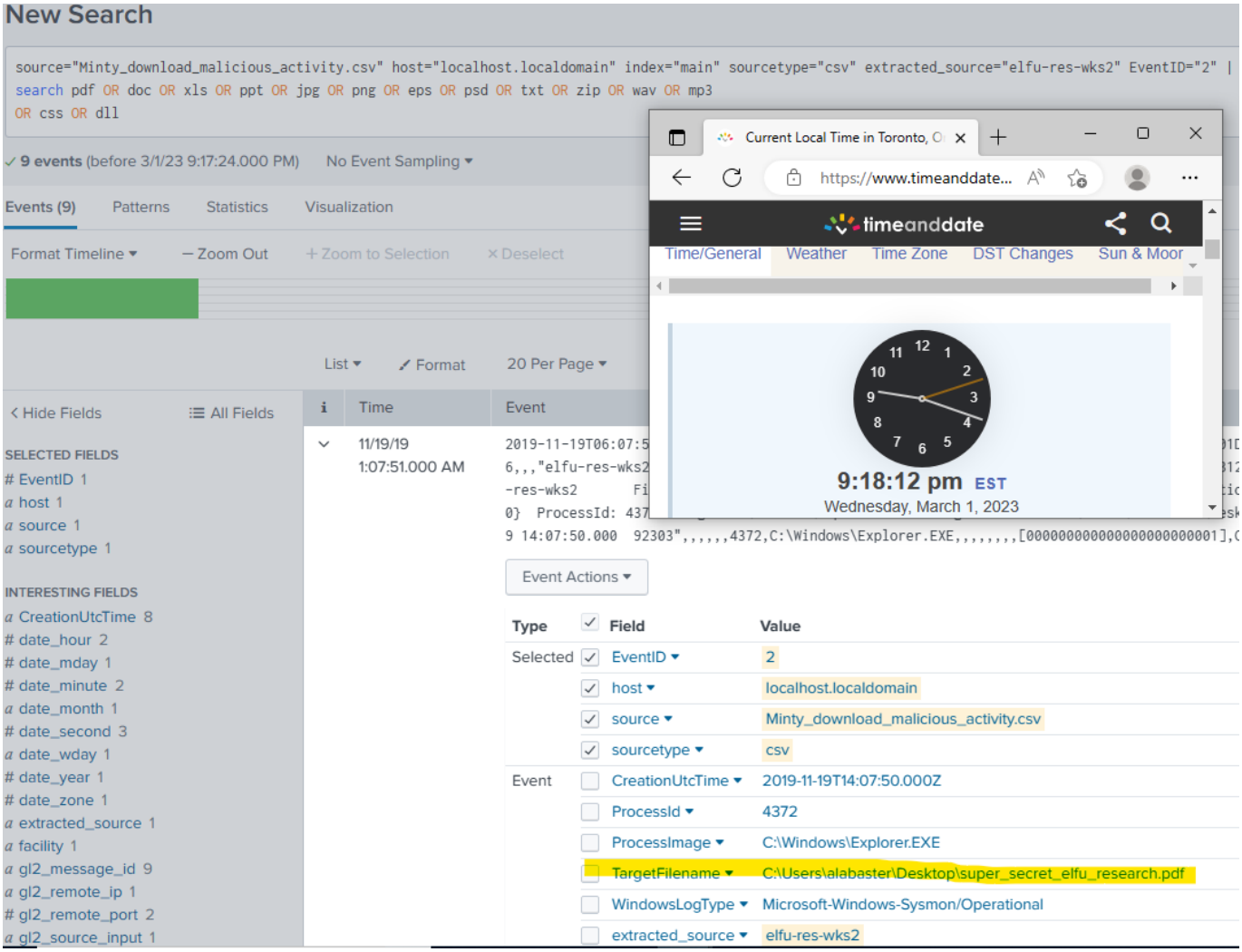


Figure 8.1

Question #5

What is the IPv4 address (as found in logs) the secret research document was exfiltrated to?

Answer

To answer this question, we first need to know everything in regards to the file we just discovered in the previous question. In order to do this, we use the “search” keyword to give us a better understand. In Figure 9 we can see that the file was being sent through PowerShell to Pastebin hence our next search query should be just that. After searching we are left with two results as shown in Figure 10. To find out which one is correct we need to identify what the Event ID is. In the second event result, it shows an Event ID=1 which is a process creation; however, no process is really created here as shown in Figure 11. Thus, using the process of elimination it must be the first option which also is confirmed when we see Event ID=3 which is making a network connection through TCP/UDP on the machine [6]. Source and destination IP address is also present since its defined in an Event ID=3 [6] which holds true as shown in Figure 12. Hence, the IPv4 address the secret research document was exfiltrated to is: **104.22.3.84**

Figure 9 ↑

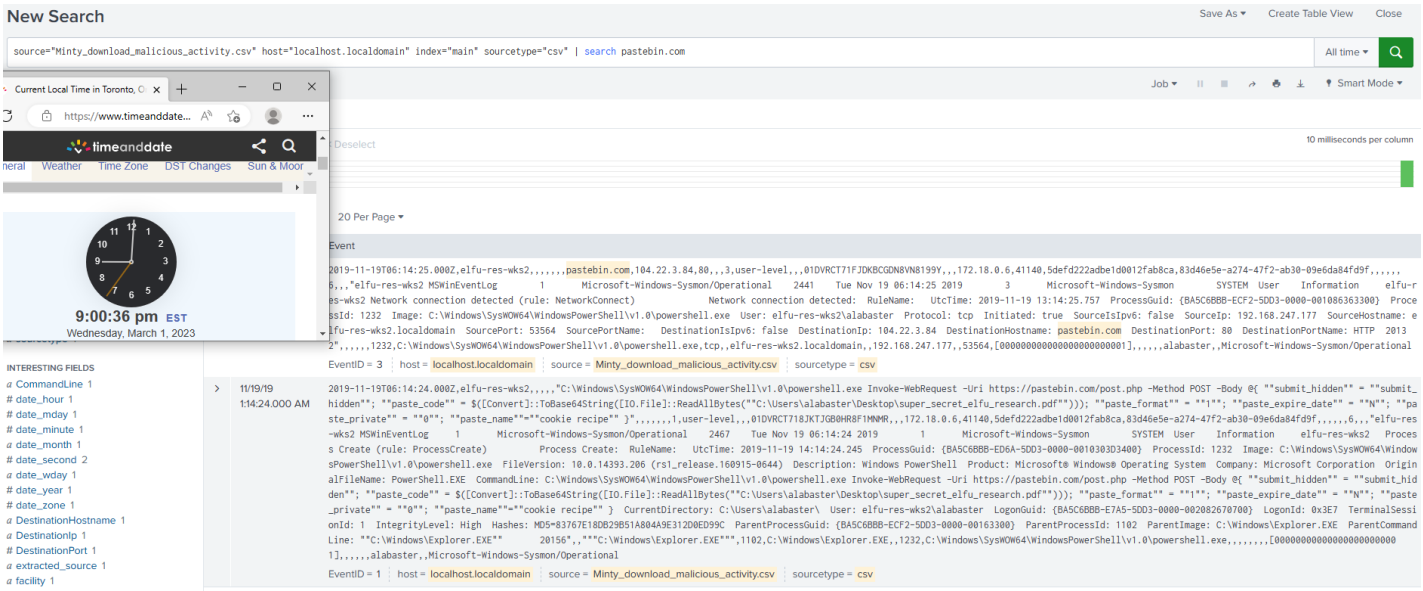


Figure 10 ↑

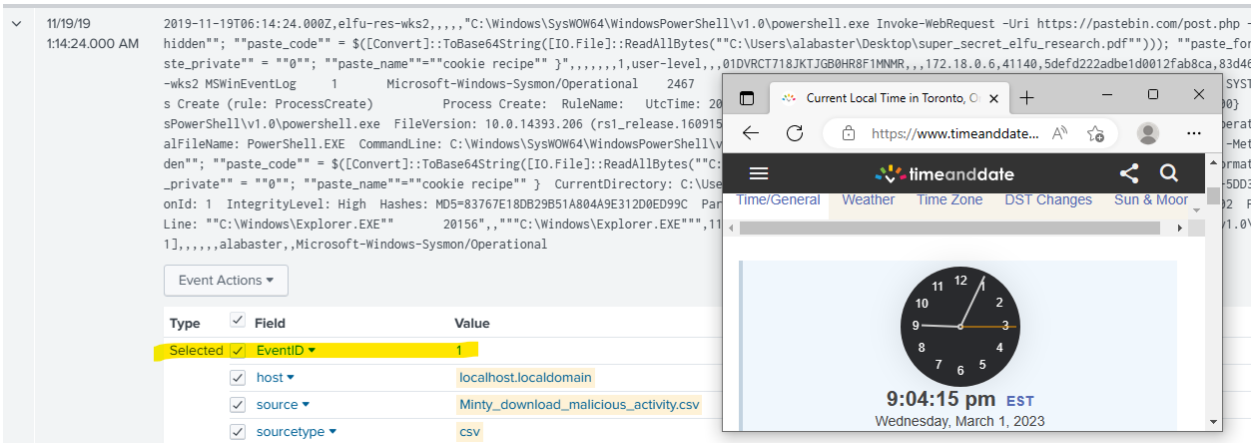


Figure 11 ↑

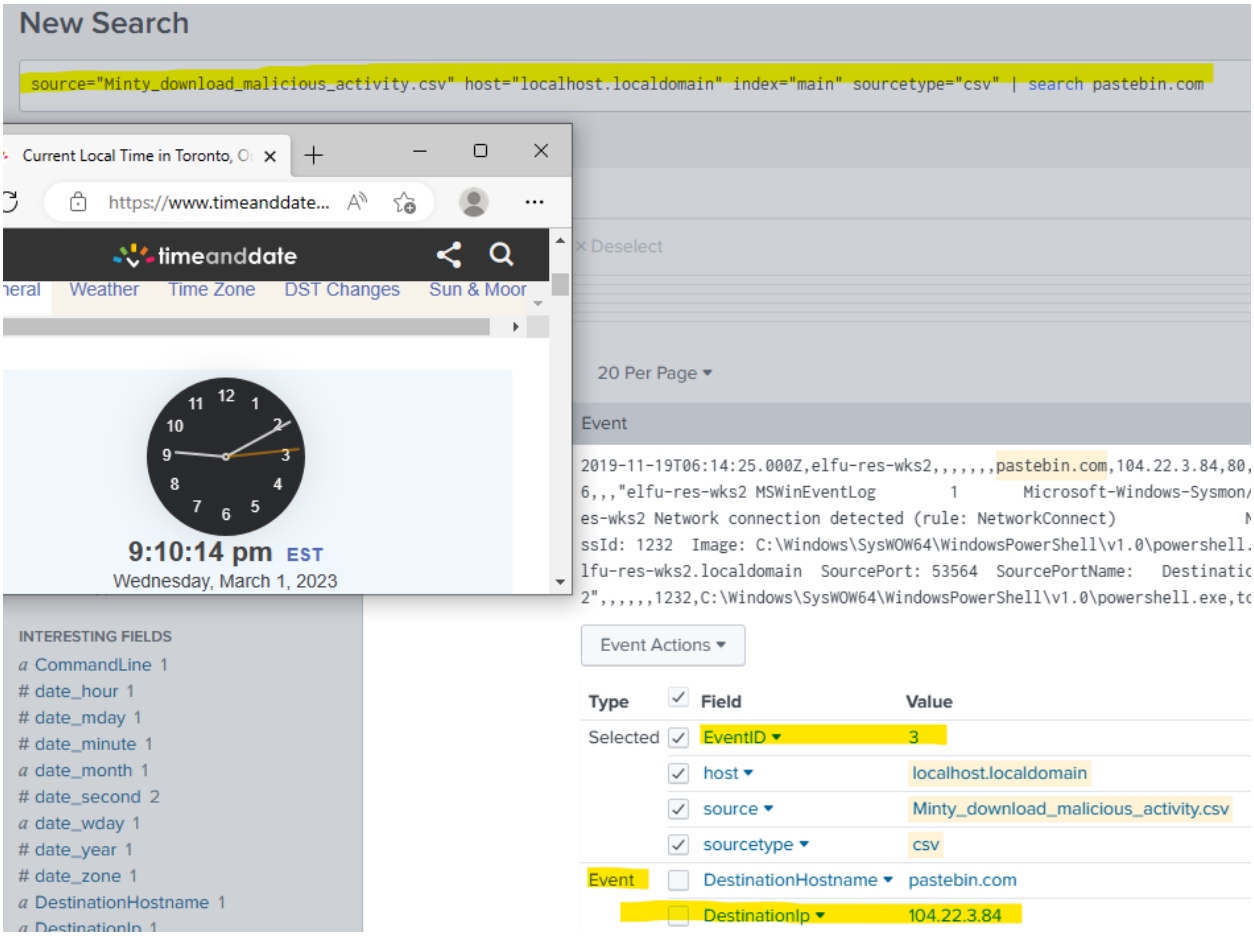


Figure 12 ↑

References

[1] P. Habibi, “Incident Response -5 Questions,” *Vimeo*, 19-Sep-2019. [Online]. Available: https://vimeo.com/609171980. [Accessed: 01-Mar-2023].

[2] “Windows Security Log Event ID 4624,” *Windows Security Log Event ID 4624 - an account was successfully logged on*. [Online]. Available: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4624#:~:text=An%20account%20was%20successfully%20logged%20on.&text=This%20event%20is%20generated%20when,system%20which%20requested%20the%20logon. [Accessed: 01-Mar-2023].

[3] “Sysmon Event ID 2,” *Sysmon event ID 2 - a process changed a file creation time*. [Online]. Available: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90002. [Accessed: 01-Mar-2023].

[4] L. Technologies, “The giant list of document file types and extensions,” *FileCenter Blog*, 18-Apr-2022. [Online]. Available: https://www.filecenter.com/blog/the-giant-list-of-document-file-types-and-extensions/. [Accessed: 01-Mar-2023].

[5] M. Russinovich and T. Garnier, “Sysmon v14.14,” *Sysmon - Sysinternals | Microsoft Learn*, 23-Jan-2023. [Online]. Available: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon. [Accessed: 01-Mar-2023].

[6] “Data Access Automation API,” *Data access automation API - Splunk Documentation*. [Online]. Available: https://docs.splunk.com/Documentation/SOAR/current/PlaybookAPI/DataAccessAPI. [Accessed: 02-Mar-2023].