Synapse Bootcamp - Module 16

Dynamic Malware Analysis - Answer Key

Dynamic Malware Analysis - Answer Key **1**
Answer Key **2**
Dynamic Malware Analysis 2
Exercise 1 Answer 2
Exercise 2 Answer 6
Exercise 3 Answer 10

© 2025 The Vertex Project, LLC

Answer Key

Dynamic Malware Analysis

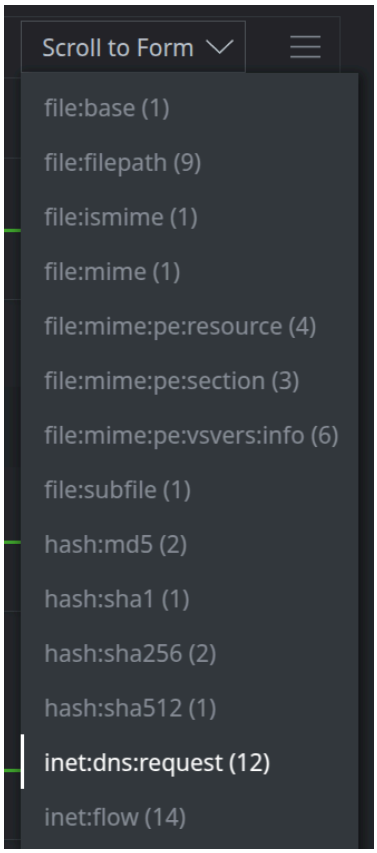
Exercise 1 Answer

Objective:

- **Use dynamic execution data to identify network activity and look for potential malware command and control (C2) communications.**

Question 1: Are there any forms that might provide us with information about **network-based** communications or command and control (C2)?

- The results include:
  - `inet:dns:request` nodes (DNS queries);
  - `inet:flow` nodes (network connections).



© 2025 The Vertex Project, LLC

> These may include **benign** activity from the sandbox but are a good place to start.

Question 2: When were the DNS queries made?

- Based on the `:time` property of the `inet:dns:request` nodes, the queries were made on multiple dates between **January 5, 2021** and **July 14, 2022** (results as of August 2025):

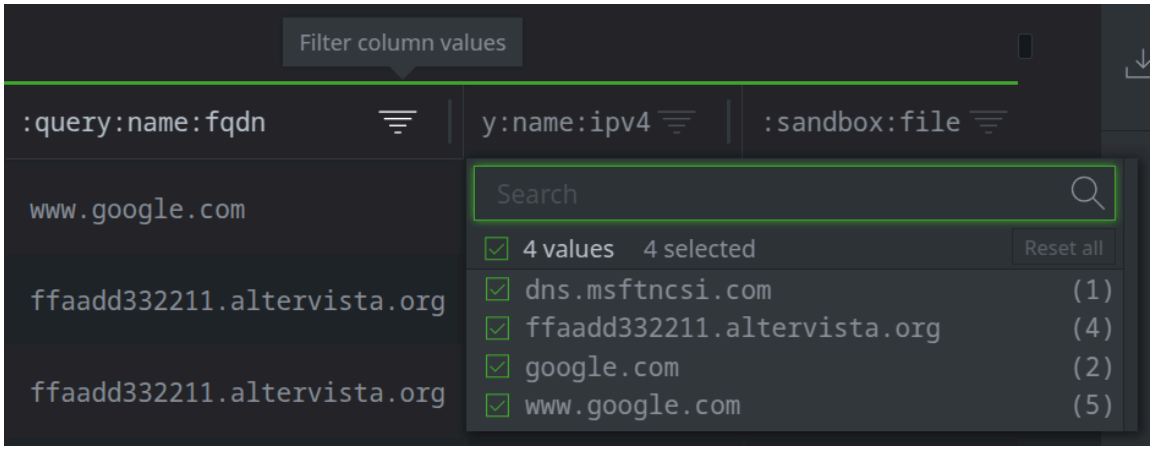
inet:dns:request (12)

	:time	:host::desc
:exe <-	2022/07/14 22:05:53	DAS-Security Orc…
:exe <-	2021/04/05 06:51:46	Tencent HABO
:exe <-	2021/01/09 12:26:39	VirusTotal Cucko…
:exe <-	2021/01/09 12:26:39	VirusTotal Cucko…
:exe <-	2021/01/05 15:52:31	Dr.Web vxCube
:exe <-	2021/01/05 15:52:31	Dr.Web vxCube
:exe <-	2021/01/05 15:52:31	Dr.Web vxCube
:exe <-	2021/01/05 12:48:46	VirusTotal Jujub…
:exe <-	2021/01/05 12:48:46	VirusTotal Jujub…

> These are the dates that the file was executed in one or more VT sandboxes.

Question 3: How many unique FQDNs were queried?

- **Four** unique FQDNs were queried during execution (as of March 2025):



Question 4: Which FQDNs (if any) would you investigate?

- The FQDN **ffaadd332211.altervista.org** is unusual and is a good place to start. Even though **altervista.org** is a legitimate hosting site, the subdomain (ffaadd332211) is unusual.

- We know the FQDN **dns.msftncsi.com** is used by Windows to check network connectivity, and **google.com/www.google.com** are well-known domains.

> **Note:** "known" FQDNs are not necessarily benign, and FQDNs that we do not recognize are not necessarily malicious. But we need to start somewhere!

Question 5: How many unique IPv4s were contacted?

- **Eleven** unique IPv4 addresses were contacted (as of August 2025):

inet:ipv4 (11)

	inet:ipv4
:dst:ipv4 ->	173.194.216.103
:dst:ipv4 ->	173.194.216.105
:dst:ipv4 ->	216.58.209.228
:dst:ipv4 ->	8.8.8.8

Question 6: Which IPv4 address (if any) is associated with FQDN **ffaadd332211.altervista.org**?

- IPv4 **88.198.107.50** is associated with FQDN **ffaadd332211.altervista.org:**

inet:dns:answer (10)

	:request::time	:a::fqdn	:a::ipv4 ↓
:request <-	2021/01/05 12:48:46	ffaadd332211.altervista.org	88.198.107.50
:request <-	2021/01/05 15:52:31	dns.msftncsi.com	131.107.255.255
:request <-	2022/07/14 22:05:53	www.google.com	142.251.42.228

> **Note:** the FQDN **ffaadd332211.altervista.org** is associated with the legitimate web hosting site **altervista.org.** This IP may be a valid AlterVista server (and not attacker-controlled infrastructure). We need to do more research to decide.

Question 7: How many files "communicate with" the FQDN?

- **Four** files communicate with the FQDN (as of May 2024):

file:bytes (4)

	file:bytes	:mime
<(refs)-	sha256:bef7c7668970c29a328dd9709c…	...
<(refs)-	sha256:500631db833b2729f784e23322…	application/vnd.mic…
<(refs)-	sha256:543e544766d13f427449596fa1…	...
<(refs)-	sha256:5973dbb7697f16df5de21073de…	...

The results include our original file (in green).

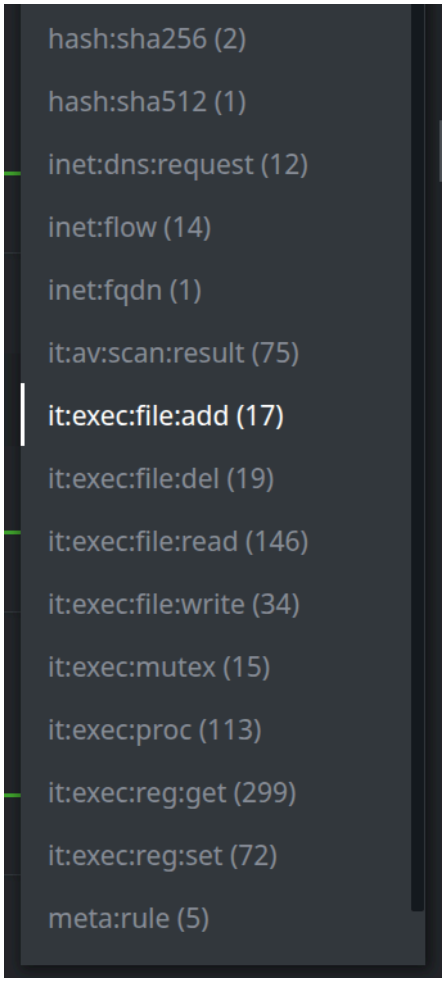
Exercise 2 Answer

Objective:

- **Use dynamic execution data to identify changes made to the host and look for additional host-based IOCs.**

Question 1: Are there any forms that might provide us with information about **host-based** activity for the file?

- The results include a number of **`it:exec:*`** nodes:



These include:

  - **`it:exec:file:*`** nodes (file system changes);
  - **`it:exec:mutex`** nodes (mutexes created in memory);
  - **`it:exec:proc`** nodes (processes or commands executed); and
  - **`it:exec:reg:*`** nodes (Windows registry changes).

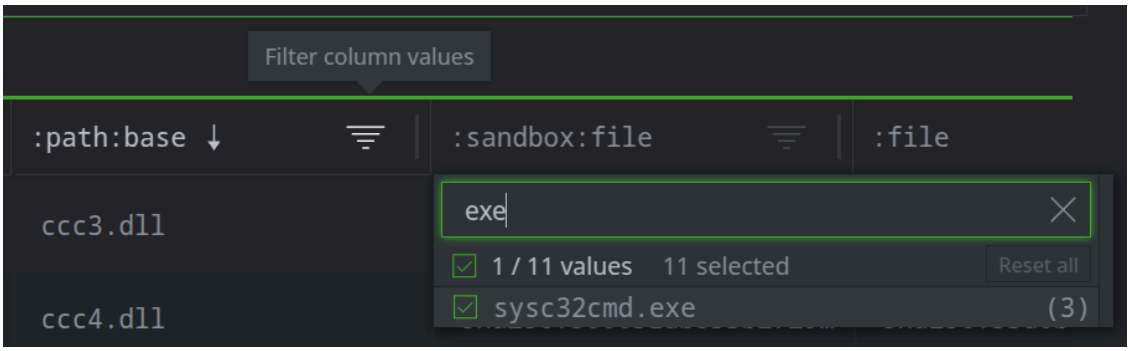
These are good places to look for host-based changes and indicators.

Question 2: Were any executable (**exe**) files added during any sandbox runs?

- A file named **sysc32cmd.exe** was added:

:file <-	2021/01/05…	Dr.Web vxC…	%homepath%/sysc32cmd.exe	sysc32cmd.exe
:file <-	2022/07/14…	DAS-Securi…	c:/users/admin/sysc32cmd.exe	sysc32cmd.exe
:file <-	2021/01/23…	VenusEye S…	c:/users/<user>/sysc32cmd.exe	sysc32cmd.exe

Tip: You can also use the **filter** feature of the **:path:base** column to browse or search for exe files:



Question 3: How many sandboxes (hosts) observed the file? When was the activity captured?

- **Three** different sandboxes observed the file **sysc32cmd.exe:**
  - Dr.Web vxCube
  - DAS-Security Orcas
  - VenusEye Sandbox

- The activity was seen on three different dates:
  - January 5, 2021 (2021/01/05)
  - July 14, 2022 (2022/07/14)
  - January 23, 2021 (2021/01/23)

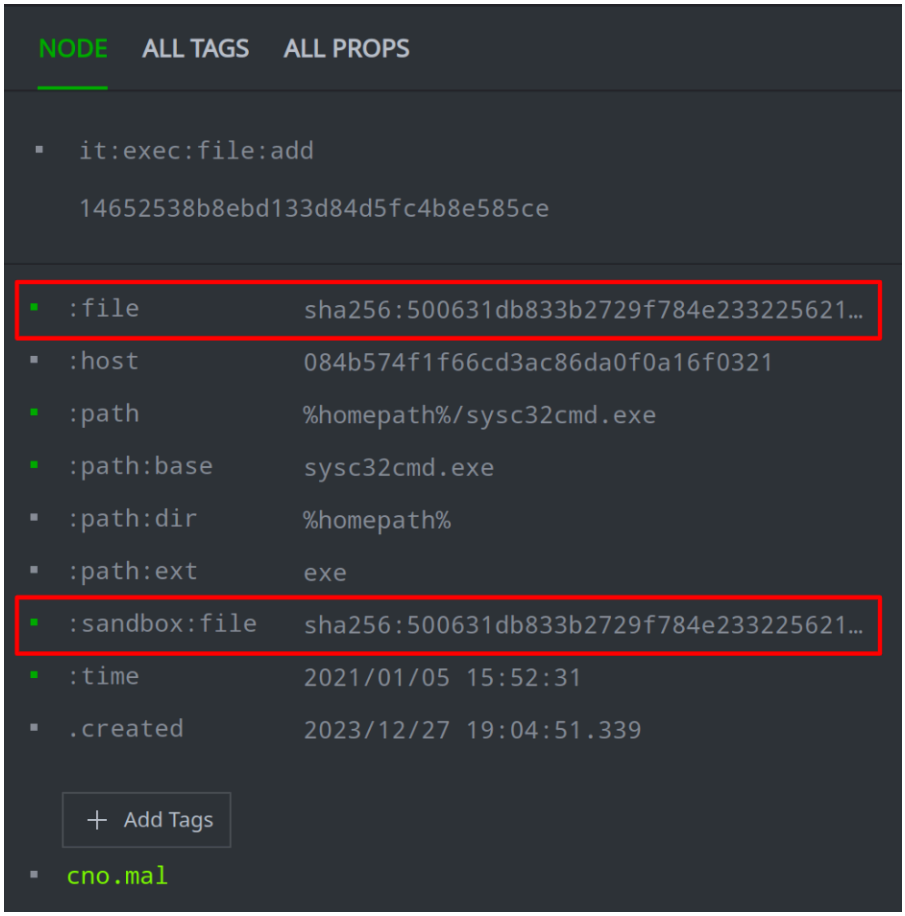
	:time	:host::desc	:path	:path:base
:file <-	2021/01/05 15:52:31	Dr.Web vxCube	%homepath%/sysc32cmd.exe	sysc32cmd.exe
:file <-	2022/07/14 22:05:53	DAS-Security Orcas	c:/users/admin/sysc32cmd.exe	sysc32cmd.exe
:file <-	2021/01/23 12:07:46	VenusEye Sandbox	c:/users/<user>/sysc32cmd.exe	sysc32cmd.exe

© 2025 The Vertex Project, LLC

This is good evidence that the file **sysc32cmd.exe** is consistently dropped (added) when our malware sample executes, and is not a sandbox artifact.

Question 4: Are the property values the same or different? What does this tell you?

- In each case, the values are **the same:**



- This tells us that the file **added** to the host has the same SHA256 hash as our original file. In other words, the malware sample **copies** itself to this location.

If the values were different, it would indicate that our original sample added ("dropped") a different (new or modified) file instead. We could investigate the new file by attempting to download the sample or retrieve other data using our Power-Ups.

© 2025 The Vertex Project, LLC

Question 5: How many **`it:exec:file:add`** nodes are in your results?

- There are **three** **`it:exec:file:add`** nodes (as of August 2025):

it:exec:file:add (3)

:time	:host::desc	:path	:path:base
2021/01/05 15:52:31	Dr.Web vxCube	%homepath%/sysc32cmd.…	sysc32cmd.exe
2022/07/14 22:05:53	DAS-Security Orcas	c:/users/admin/sysc32…	sysc32cmd.exe
2021/01/23 12:07:46	VenusEye Sandbox	c:/users/<user>/sysc3…	sysc32cmd.exe

---

Question 6: Did your query identify any **new** files that write to the same path?

- **No.** All of the results are from our original file (`file:bytes=sha256:500631db833b2729f784e233225621ddff411d7da49bd82cfd51a49b9600438f`).

Exercise 3 Answer

Objective:
- **View host-specific (sandbox-specific) execution data associated with a file.**

Question 1: How many hosts (sandboxes) recorded DNS queries during file execution?

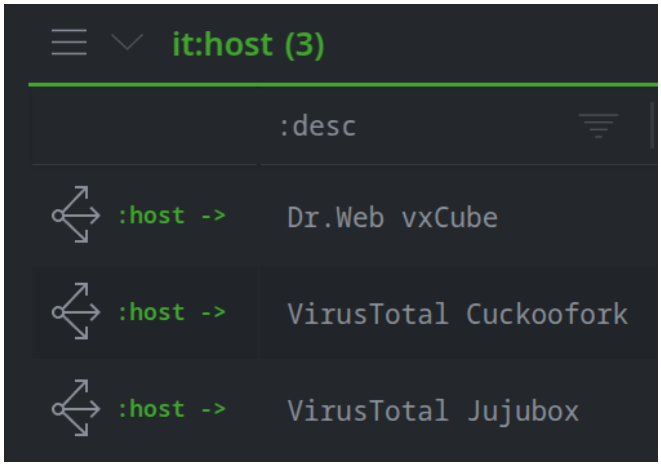
- **Five** sandboxes recorded DNS query data (as of August 2025):

it:host (5)

	:desc
:host ->	VirusTotal Jujubox
:host ->	Dr.Web vxCube
:host ->	VirusTotal Cuckoofork
:host ->	DAS-Security Orcas
:host ->	Tencent HABO

Question 2: How many hosts (sandboxes) recorded DNS queries for our C2 FQDN?

- **Three** sandboxes recorded DNS queries for that FQDN:



Question 3: Was the DNS information captured by the sandboxes identical? If not, how do they differ?

- **No,** the information recorded was **not identical.**
  - **Both** sandboxes captured the query to **ffaadd332211.altervista.org**.
  - Each sandbox captured a **different** query for Google (**google.com** vs **www.google.com**).
  - **Only** the Dr.Web sandbox captured the query for **dns.msftncsi.com.**

Different sandbox environments can produce very different results, based on many factors. These include the sandbox configuration (OS and applications), how the sandbox is instrumented, and whether the sandbox has a 'live' Internet connection.

Synapse gives you the "best of both worlds" - you can view:

- **all** sandbox activity associated with a file ("show me all the things associated with this file's execution in **any** environment")
- activity from a **specific** sandbox ("show me what happens when this sample is executed by Vendor X")

Comparing the two may help distinguish activity associated with the malware itself from activity that is incidental or represents artifacts from a particular sandbox environment.

© 2025 The Vertex Project, LLC