5. Interesting Logs to Look at

The following is not a complete list, it just serves as a good starting point. Interesting Logs and events to look at:

5.1. Accounts Related

ID	Description	EVTX File
4624	An account was successfully logged on	Security
4625	An account failed to log on	Security
4634	An account was logged off	Security
4720	A user account was created	Security
4722	A user account was enabled	Security
4725	A user account was disabled	Security
4726	A user account was deleted	Security
4728	A member was added to a security-enabled global group	Security
4732	A member was added to a security-enabled local group	Security
4738	A user account was changed	Security
4781	The name of an account was changed	Security

5.2. Boot, hibernation, shutdown

ID	Description	EVTX File
4608	Windows is starting up	Security
4647	User initiated logoff	Security
1074	Shutdown	System
423	The system is entering sleep	System
6005	The event logging service was started	System

ID	Description	EVTX File
60084	Unexpected Shutdown	System
6009	System Boot	System

5.3. Password

ID	Description	EVTX File
4723	An attempt was made to change an account’s password	Security
4724	An attempt was made to reset an account’s password	Security

5.4. Software Installation

ID	Description	EVTX File
11707	Product installed	Application
11708	Product installed failed	Application

5.5. Windows Update

ID	Description	EVTX File
19	Installation Successful: Windows successfully installed the following update …	System
43	Installation Started: Windows has started installing the following update …	System
44	Windows Update started downloading an update …	System

In what kind of scenarios do you think it would be good to look at the above logs?

6. Your tasks for this week

Below are your tasks that you should complete by next week, where we will discuss the results together.