Part A:

(a) Logon Success:

Time	fields.hostname	event.code	event.action
Oct 8, 2020 @ 16:14:20.402	_309555015	4,624	logged-in

This is exactly the log generated when I signed in my windows 10. The “sign in” event code was 4624, and the event action field showed “logged-in”.

t log.level	資訊
t message	› 帳戶已順利登入。 主體: 安全性識別碼: S-1-5-18 A帳戶名稱: DCSLAB-HC$ 帳戶網域: WORKGROUP 登入識別碼: 0x3E7
t process.executable	C:\Windows\System32\svchost.exe
t process.name	svchost.exe
# process.pid	1,596
t related.user	HC, DCSLAB-HC$
t source.domain	DCSLAB-HC
t source.ip	127.0.0.1
# source.port	0
t tags	beats_input_codec_plain_applied

As you can see, the message shows “The account has been successfully logged in“. And the managed process is “svchost.exe”. You can also see the information about computer, such as user, domain, ip, port.

(b) Logoff:

Time	fields.hostname	event.code	event.action
Oct 8, 2020 @ 16:14:20.403	_309555015	4,634	logged-out

This is exactly the log generated when I logged out my windows 10. The “sign out” event code was 4634, and the event action field showed “logged-out”.

t message	帳戶已登出。 主旨: 安全性識別碼: S-1-5-21-4153427879-829393052-2419649850-1001 帳戶名稱: HC 帳戶網域: DCSLAB-HC 登入識別碼: 0x62DA7DD 登入類型: 2 當登入工作階段損毀時，就會產生這個事件。這個事件可能與使用登入識別碼數值的登入事件正面相關。登入識別碼僅有在重新啟動相同電腦之間才會是唯一的。
t related.user	HC
t tags	beats_input_codec_plain_applied

As you can see, the message shows “The account has been logged out“. You can also see the information about computer, such as user, domain, login ID.

(e) Open the specific application:

Time	fields.hostname	event.code	event.action
Oct 8, 2020 @ 16:08:28.895	_309555015	4,688	created-process

This is exactly the log generated when I opened the Calculator.exe. Because opening an application has to create a process, the corresponding event code was 4688, and the event action field showed “created-process”.

t log.level	資訊
t message	已建立新的處理程序。 建立者主體: 安全性識別碼: S-1-5-18 帳戶名稱: DCSLAB-HC$ 帳戶網域: WORKGROUP 登入識別碼: 0x3E7
t process.executable	C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.2008.2.0_x64__8wekyb3d8bbwe\Calculator.exe
t process.name	Calculator.exe
t process.parent.executable	C:\Windows\System32\svchost.exe
t process.parent.name	svchost.exe
# process.pid	6,444
t related.user	DCSLAB-HC$, HC
t tags	beats_input_codec_plain_applied

As you can see, the message shows “New process has been created“. And the executed process is “Calculator.exe”, its parent process is “svchost.exe”. You can also see the information about computer, such as user, domain, login ID.

(g) Create file:

Time	fields.hostname	event.code	event.action
Oct 8, 2020 @ 16:25:54.444	_309555015	4,656	SAM

This is exactly the log generated when I create a new file. Because creating a new object has to request object control code, the corresponding event code was 4656, and the event action field showed “SAM” which is security account manager. It can be used to authenticate local and remote users. Beginning with Windows 2000 SP4, Active Directory authenticates remote users. SAM uses cryptographic measures to prevent unauthenticated users accessing the system.

t log.level	資訊
t message	已要求物件控制代碼。 主體: 安全性識別碼: S-1-5-18 帳戶名稱: DCSLAB-HC$ 帳戶網域: WORKGROUP 登入識別碼: 0x3E7
t tags	beats_input_codec_plain_applied

As you can see, the message shows “Object control code requested“. You can also see the information about computer, such as user, domain, login ID.

(ii) DNS query:

Time	fields.hostname	event.code	event.action
Oct 8, 2020 @ 16:34:40.302	_309555015	-	-

This is exactly the log generated when I type the command “nslookup youtube.com" in PowerShell. Because packetbeat doesn’t send the event code and event action, these two fields are empty.

@timestamp	Oct 8, 2020 @ 16:34:40.302
@version	1
_id	MuJZB3UBkCXOYSS1Gdv2
_index	logstash-_309555015.packetbeat
_score	-
_type	_doc
agent.ephemeral_id	3eaa972c-614d-4382-bbe0-2391924e7592
agent.hostname	DCSLAB-HC
agent.id	f3dd4926-3336-4fc1-8272-88a52a087904
agent.name	_309555015
agent.type	packetbeat
agent.version	7.9.2
client.bytes	29
client.ip	140.113.207.36
client.port	64,723
destination.bytes	312
destination.ip	140.113.1.1
destination.port	53
dns.additionals_count	8
dns.answers	{ "class": "IN", "type": "AAAA", "name": "youtube.com", "data": "2404:6800:4008:803::200e", "ttl": "249" }
dns.answers_count	1
dns.authorities_count	4

dns.flags.authentic_data	false
dns.flags.authoritative	false
dns.flags.checking_disabled	false
dns.flags.recursion_available	true
dns.flags.recursion_desired	true
dns.flags.truncated_response	false
dns.header_flags	RD, RA
dns.id	3
dns.op_code	QUERY
dns.question.class	IN
dns.question.etld_plus_one	youtube.com
dns.question.name	youtube.com
dns.question.registered_domain	youtube.com
dns.question.top_level_domain	com
dns.question.type	AAAA
dns.resolved_ip	2404:6800:4008:803::200e
dns.response_code	NOERROR
dns.type	answer
ecs.version	1.5.0
event.category	network_traffic, network
event.dataset	dns
event.duration	2,389,000
event.end	Oct 8, 2020 @ 16:34:40.304
event.kind	event
event.start	Oct 8, 2020 @ 16:34:40.302
event.type	connection, protocol

fields.hostname	_309555015
fields.logtag	packetbeat
host.architecture	x86_64
host.hostname	DCSLAB-HC
host.id	3d2dfedb-517a-4645-8bdf-d5427c5b78c8
host.ip	fe80::d0f2:8fde:4876:ba49, 192.168.56.1, fe80::a1e1:9a4e:7eaa:9394, 140.113.207.36
host.mac	0a:00:27:00:00:0d, 74:d4:35:8d:89:da
host.name	_309555015
host.os.build	17763.1457
host.os.family	windows
host.os.kernel	10.0.17763.1457 (WinBuild.160101.0800)
host.os.name	Windows 10 Education
host.os.platform	windows
host.os.version	10.0
method	QUERY
network.bytes	341
network.community_id	1:MoFFfHhuYgGdOR6Ht3taDCV3dMA=
network.direction	outbound
network.protocol	dns
network.transport	udp
network.type	ipv4
query	class IN, type AAAA, youtube.com
related.ip	140.113.207.36, 140.113.1.1, 2404:6800:4008:803::200e
resource	youtube.com
server.bytes	312
server.ip	140.113.1.1
server.port	53

As you can see, the query name is “youtube.com“. And the client ip is “140.113.207.36”, which is my computer static ip. You can also see the information about query, such as client, destination, server, dns, query and so on.

How I found these correspondences?

It’s very easy. Because every event in windows 10 has a specific event code, you just need to search for the corresponding code. The only scenario that took my much time is “create a new file”. I didn’t know there’s no event action called “create a file”, so I ignored that right event action called “SAM” in the beginning. Whenever you create a new file or folder, you have to request an object control code. And the event’s corresponding event code is 4656.

Part B:

Problems I encountered while using the ELK stack:

1. **Kibana server login account**
   Solution: I found a login account in “docker-compose.yml”.
   Username: kinbanaserver
   Password: admin
2. **Windows 10 on my local computer cannot connect to the virtual machine Ubuntu server**
   Solution: You have to set the network port forwarding from local virtual box host-only network to virtual machine local network.
3. **There’s no any output in my ELK docker**
   Solution: You have to comment Elasticsearch output and change output to logstash in “winlogbeat.yml” or “packetbeat.yml”.
4. **My log had sent to logstash but I cannot see anything on my kibana web page**
   Solution: You have to create a new index pattern called “logstash*” in your account.
   And you also have to open “secpol.msc”, you can go to local policies/audit policy. Activate Success on “Audit process tracking” and you will get an event log entry in the security event log every time a process starts or ends. If you want to see the object-related events, you have to activate success on “Audit object access”
5. **I can’t create a new index pattern called “logstash*” in my account!!!** ★★★★
   Solution: I found there’s a lot of accounts in kibana, and all of them have different permissions. Unfortunately, the “kibanaserver” account is a trap, it is useless to help me create the Index pattern called “logstash*”. I wasted a lot of time to figure out this problem. Finally, I saw that the “admin” account has all permissions. And I successfully created “logstash*” in this account. Hey, TA, I found this account on my own. Next time, you have to remind us earlier, or don’t remind anything.
6. **Packetbeat cannot start**
   Solution: Before you begin, download and install a packet sniffing library, such as Npcap, that implements the libpcap interfaces.
7. **Log showed on kibana whose field.hostname is “unknown”**
   Solution: You have to add hostname value under fields in “winlogbeat.yml” or “packetbeat.yml”.
8. **How to check if the event code is right?**
   Solution: I found a website with an event code list for windows.
   https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx?i=j