



Aim and Objectives

```
graph TD; Aim[Aim : Analyse ransomware attacks and demonstrate forensic investigation techniques.]; Objectives[Objectives:]; Review[Review the evolution and impact of ransomware.]; Case[Examine real-world case studies (WannaCry, Ryuk, Colonial Pipeline).]; Simulate[Simulate and analyse a ransomware attack in a virtual machine.]; Mitigation[Propose effective mitigation strategies.]; Objectives --- Review; Objectives --- Case; Objectives --- Simulate; Objectives --- Mitigation;
```

Aim : Analyse ransomware attacks and demonstrate forensic investigation techniques.

Objectives:

- Review the evolution and impact of ransomware.
- Examine real-world case studies (WannaCry, Ryuk, Colonial Pipeline).
- Simulate and analyse a ransomware attack in a virtual machine.
- Propose effective mitigation strategies.

```
graph TD; Start[Start] --> VM[VM Creation]; VM --> Tools[Tool Installation]; Tools --> Infect[Infect VM Ransomware]; Infect --> Collect[Artefact Collection]; Collect --> Volatility[Volatility]; Collect --> FTK[FTK Imager]; Collect --> Wireshark[Wireshark]; Volatility --> REM[REMnux Analysis]; FTK --> Flare[Flare VM Analysis]; Wireshark --> Cuckoo[Cuckoo Sandbox]; REM --> Correlate[Result Correlation & Logging]; Flare --> Correlate; Cuckoo --> Correlate;
```

The flowchart illustrates the proposed methodology for ransomware analysis. It begins with 'Start', followed by 'VM Creation', 'Tool Installation', and 'Infect VM Ransomware'. The process then moves to 'Artefact Collection', which branches into three parallel analysis steps: 'Volatility', 'FTK Imager', and 'Wireshark'. These steps lead to 'REMnux Analysis', 'Flare VM Analysis', and 'Cuckoo Sandbox' respectively. Finally, all three analysis results feed into 'Result Correlation & Logging'.

[illegible]

C:\MINGW64\Users\Tester\volatility											
4180	878	5660	msedge.exe	0xc02231f58080	18	-	1	False	2025-07-16 08:26:152.000000 UTC	N/A	Disabled
4180	5660	msedge.exe	0xc02231f58080	18	-	-	1	False	2025-07-16 08:27:24.000000 UTC	N/A	Disabled
4180	5660	msedge.exe	0xc02231f58080	18	-	-	1	False	2025-07-16 08:27:33.000000 UTC	N/A	Disabled
4334	784	httr.exe	0xc02231f58080	0	-	-	1	False	2025-07-16 08:31:08.000000 UTC	2025-07-16 08:31:08.000000 UTC	Disabled
4218	784	httr.exe	0xc02231f58080	0	-	-	1	False	2025-07-16 08:37:23.000000 UTC	2025-07-16 08:37:27.000000 UTC	Disabled
4218	784	httr.exe	0xc02231f30800	0	-	-	1	False	2025-07-16 08:37:15.000000 UTC	2025-07-16 08:37:15.000000 UTC	Disabled
7648	784	httr.exe	0xc02231f58080	0	-	-	1	False	2025-07-16 08:48:109.000000 UTC	2025-07-16 08:48:18.000000 UTC	Disabled
7664	784	httr.exe	0xc02231f58080	0	-	-	1	False	2025-07-16 08:48:41.000000 UTC	2025-07-16 08:48:44.000000 UTC	Disabled
5960	5660	svchost.exe	0xc02231f58080	4	-	0	False	2025-07-16 08:48:142.000000 UTC	N/A	Disabled	
5960	5660	svchost.exe	0xc02231f58080	15	-	0	False	2025-07-16 08:48:1450.000000 UTC	N/A	Disabled	
4060	784	httr.exe	0xc02231f58080	0	-	-	1	False	2025-07-16 08:56:137.000000 UTC	2025-07-16 08:56:120.000000 UTC	Disabled
1066	784	httr.exe	0xc02231f58080	0	-	-	1	False	2025-07-16 08:56:147.000000 UTC	2025-07-16 08:56:147.000000 UTC	Disabled
7528	784	httr.exe	0xc02231f58080	0	-	-	1	False	2025-07-16 09:03:118.000000 UTC	2025-07-16 09:03:17.000000 UTC	Disabled
7812	664	svchost.exe	0xc02231f54080	3	-	0	False	2025-07-16 09:04:131.000000 UTC	N/A	Disabled	
9060	664	svchost.exe	0xc02231f54080	1	-	0	False	2025-07-16 09:04:141.000000 UTC	N/A	Disabled	
7476	784	winPRVSE.exe	0xc02231f340	3	-	0	False	2025-07-16 09:05:155.000000 UTC	N/A	Disabled	
4024	664	svchost.exe	0xc02231f54080	4	-	0	False	2025-07-16 09:05:131.000000 UTC	N/A	Disabled	
7484	664	svchost.exe	0xc02231f54080	8	-	0	False	2025-07-16 09:05:134.000000 UTC	N/A	Disabled	
4888	784	httr.exe	0xc02231f5e080	0	-	-	1	False	2025-07-16 09:08:118.000000 UTC	2025-07-16 09:08:25.000000 UTC	Disabled
6932	784	httr.exe	0xc02231f5e080	0	-	-	1	False	2025-07-16 09:08:148.000000 UTC	2025-07-16 09:08:149.000000 UTC	Disabled
306	1456	comhost.exe	0xc02231f20800	0	-	-	1	False	2025-07-16 09:09:010.000000 UTC	2025-07-16 09:09:03.000000 UTC	Disabled
6552	4148	SearchProtocol	0xc02231f6080	7	-	0	False	2025-07-16 09:10:40.000000 UTC	N/A	Disabled	
738	204	msedge.exe	0xc02231f58080	3	-	0	False	2025-07-16 09:12:02.000000 UTC	N/A	Disabled	
4004	4148	SearchProtocol	0xc02231f6080	8	-	0	False	2025-07-16 09:12:139.000000 UTC	N/A	Disabled	
718	784	httr.exe	0xc02231f39080	0	-	-	1	False	2025-07-16 09:12:236.000000 UTC	2025-07-16 09:12:22.000000 UTC	Disabled
9132	784	RuntimeBroker	0xc02231f6e080	6	-	-	1	False	2025-07-16 09:12:236.000000 UTC	N/A	Disabled
4036	784	RuntimeBroker	0xc02231f6e080	6	-	-	1	False	2025-07-16 09:12:244.000000 UTC	N/A	Disabled
6386	4932	comhost.exe	0xc02231f6080	7	-	0	False	2025-07-16 09:12:246.000000 UTC	N/A	Disabled	
1928	4										