

Cyber Law and Forensics (CS402)

Practical Exam (26-Apr-2023)

U19CS012

A.) Answer the Following Questions from the Given Evidence Files:



(1) Identify the commands that were typed in RUN dialogue box.

HKCU(ntuser.dat)\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

-> \RunMRU Shows MRU (Most Recent Used) run command

1. Default - Nothing Found

(C:\Users\Admin\Desktop\CLF_Practical_Exam\C\Users\Default)

CLF_Practical_Exam > C > Users > Default				
<input type="checkbox"/> Name	Date modified	Type	Size	
 AppData	24-Apr-23 11:12 AM	File folder		
<input checked="" type="checkbox"/>  NTUSER.DAT	18-Jan-23 12:14 PM	DAT File	256 KB	
<input type="checkbox"/> NTUSER.DAT.LOG1	07-May-22 10:47 AM	LOG1 File	8 KB	
<input type="checkbox"/> NTUSER.DAT.LOG2	07-May-22 10:47 AM	LOG2 File	0 KB	

2. HP - Found

Tool Used:

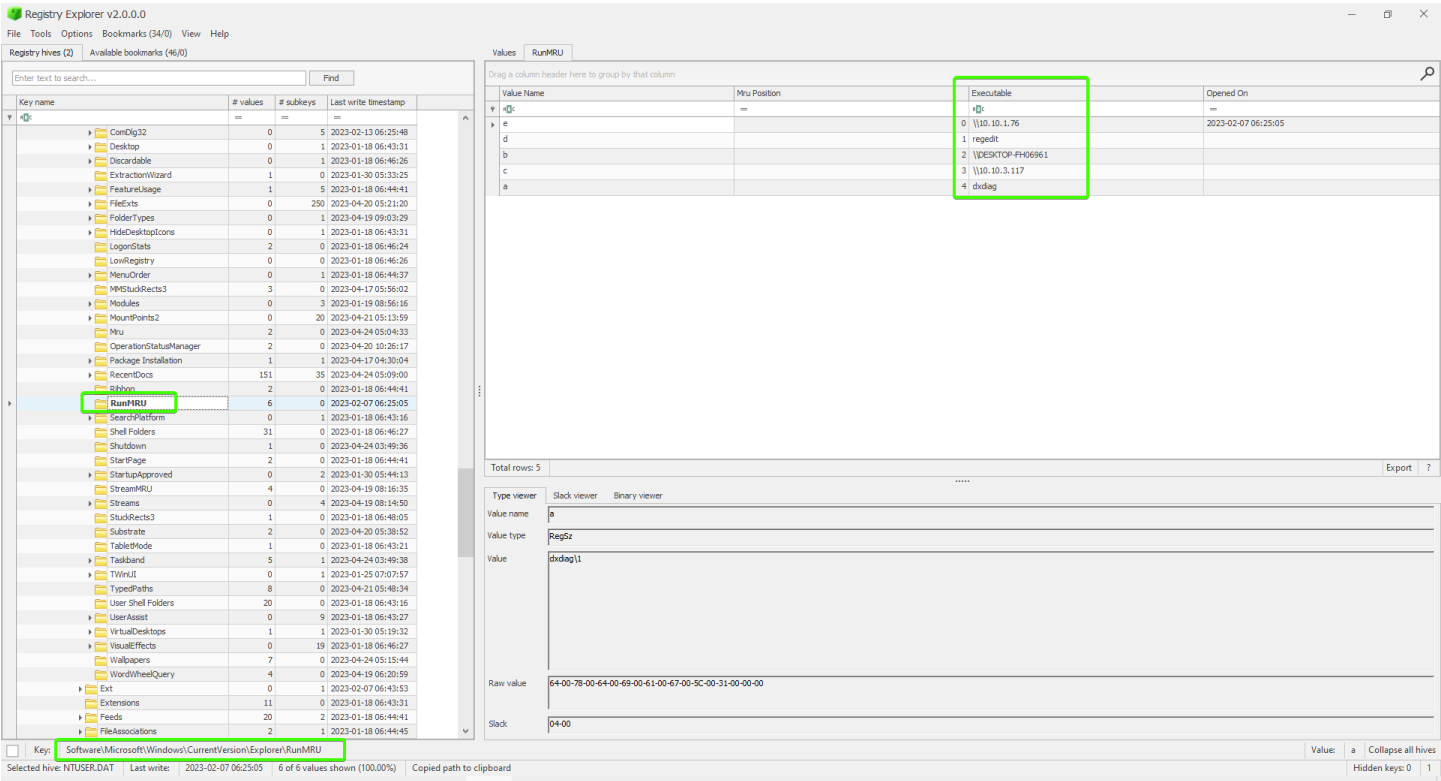
Registry Explorer by Eric Zimmerman

File Used:

NTUSER.DAT

Location:

C:\Users\Admin\Desktop\CLF_Practical_Exam\C\Users\HP\NTUSER.DAT



Executable	
	A B C
0	\\10.10.1.76
1	regedit
2	\\DESKTOP-FH06961
3	\\10.10.3.117
4	dxdiag

Path

Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Final Answer:

	Executable
	ABC
0	\\10.10.1.76
1	regedit
2	\\DESKTOP-FH06961
3	\\10.10.3.117
4	dxdiag

(2) When the log_tempering.csv was last opened?

Tool Used:

Registry Explorer by Eric Zimmerman

File Used:

NTUSER.DAT

Location:

C:\Users\Admin\Desktop\CLF_Practical_Exam\C\Users\HP\NTUSER.DAT

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (34/0) View Help

Registry hives (2) Available bookmarks (46/0)

Enter text to search... Find

Key name # values # subkeys Last write timestamp

Modules 0 3 2023-01-19 08:56:16

MountPoints2 0 20 2023-04-21 05:13:59

Mru 2 0 2023-04-24 05:04:33

OperatorStatusManager 2 0 2023-04-20 10:26:17

RecentDocs 151 35 2023-04-21 04:30:04

AutomaticDestinations-ms 2 0 2023-04-19 05:56:53

.csv 19 0 2023-04-21 05:33:42

.datt 2 0 2023-04-18 09:10:44

.dd 2 0 2023-04-12 08:44:02

.doc 7 0 2023-04-21 05:44:23

.docx 21 0 2023-04-24 05:03:18

.E01 2 0 2023-02-13 06:41:14

.evtx 2 0 2023-02-01 09:02:36

.html 4 0 2023-03-24 08:25:07

.hve 2 0 2023-04-18 09:18:52

.ISO 3 0 2023-04-18 10:00:29

.jpg 16 0 2023-04-21 06:07:54

.log 2 0 2023-04-18 09:18:49

.mp4 21 0 2023-04-05 10:25:32

.ova 2 0 2023-01-18 06:43:27

.ovf 2 0 2023-03-24 03:51:37

.pdf 21 0 2023-04-24 03:50:04

.png 21 0 2023-02-01 06:15:45

.PolicyRules 2 0 2023-02-08 09:23:34

.pot 2 0 2023-04-11 04:50:46

.pptx 17 0 2023-04-21 05:16:33

.ps1 2 0 2023-02-08 09:01:43

.raw 2 0 2023-04-17 09:31:05

.TS 9 0 2023-03-23 05:56:16

.tsv 2 0 2023-04-19 08:22:00

.tbt 20 0 2023-04-24 05:05:13

.vhdx 4 0 2023-04-21 05:13:58

.vmx 2 0 2023-01-18 06:43:27

.webm 17 0 2023-03-29 06:24:27

.xls 3 0 2023-02-24 06:52:55

.xlsx 17 0 2023-04-21 06:08:18

.x01 2 0 2023-01-20 09:18:19

.zip 21 0 2023-04-20 10:10:30

Folder 31 0 2023-04-24 05:09:00

Ribbon 2 0 2023-01-18 06:44:41

RunMRU 6 0 2023-02-07 06:25:05

Values Recent documents

Drag a column header here to group by that column

Extension	Value Name	Target Name	Link Name	Mru Position	Opened On	Extension Last Opened
.csv	log_tampering.csv	log_tampering.csv	log_tampering.csv.link		2023-04-21 05:33:42	
.csv	lateral_movement.csv	lateral_movement.csv	lateral_movement.csv.link	1		
.csv	antivirus.csv	antivirus.csv	antivirus.csv.link	2		
.csv	account_tampering.csv	account_tampering.csv	account_tampering.csv.link	3		
.csv	login_attacks.csv	login_attacks.csv	login_attacks.csv.link	4		
.csv	2023-04-20T05_08_53_2320964_CopyLog.csv	2023-04-20T05_08_53_2320964_CopyLog.csv	2023-04-20T05_08_53_2320964_CopyLog.csv.link	5		
.csv	20230419134019_Windows10C_1_DESKTOP-PRJFDQP_AppCompacache.csv	20230419134019_Windows10C_1_DESKTOP-PRJFDQP_AppCompacache.csv	20230419134019_Windows10C_1_DESKTOP-PRJFDQP_AppCompacache.csv.link	6		
.csv	20230419054808_LECmd_Output.csv	20230419054808_LECmd_Output.csv	20230419054808_LECmd_Output.csv.link	7		
.csv	20230419054433_LECmd_Output.csv	20230419054433_LECmd_Output.csv	20230419054433_LECmd_Output.csv.link	8		
.csv	2023-04-18T11_23_38_1755991_CopyLog.csv	2023-04-18T11_23_38_1755991_CopyLog.csv	2023-04-18T11_23_38_1755991_CopyLog.csv.link	9		
.csv	2023-04-18T11_23_38_1755991_SlipLog.csv	2023-04-18T11_23_38_1755991_SlipLog.csv	2023-04-18T11_23_38_1755991_SlipLog.csv.link	10		
.csv	2023-04-18T11_15_58_1433601_CopyLog.csv	2023-04-18T11_15_58_1433601_CopyLog.csv	2023-04-18T11_15_58_1433601_CopyLog.csv.link	11		
.csv	Evidence 2-365-InteractiveSignline_2022-02-01_2022-02-08.csv	Evidence 2-365-InteractiveSignline_2022-02-01_2022-02-08.csv	Evidence 2-365-InteractiveSignline_2022-02-01_2022-02-08.csv.link	12		
.csv	Security.csv	Security.csv	Security.csv.link	13		
.csv	Open Alerts.csv	Open Alerts.csv	Open Alerts.csv.link	14		
.csv	sigma.csv	sigma.csv	sigma.csv.link	15		
.csv	sample.csv	sample.csv	sample.csv.link	16		

Total rows: 18

Type viewer Slack viewer

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23

00000000 66 00 69 00 6C 00 65 00 2E 00 63 00 73 00 76 00 00 00 5A 00 32 00 00 00 00 00 00 00 00 66 69 6C 65

00000024 2E 6C 6E 6B 00 00 42 00 09 00 04 00 EF BE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000048 00

0000006C 00 00

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Data interpreter ?

Value: 0 Collapse all hives

Hidden keys: 0 1

Path

System (HKLM) \ Software \ Microsoft \ Windows \ Current Version \ RecentDocs

Final Answer:

2023-04-21 05:33:42

(3) Identify USB devices attached to the system.

Tool Used:

USB Detective

File Used:

1. SYSTEM Hive
(C:\Users\Admin\Desktop\CLF_Practical_Exam\C\Windows\System32\config)
2. SOFTWARE Hive
(C:\Users\Admin\Desktop\CLF_Practical_Exam\C\Windows\System32\config)
3. NTUSER.DAT Hive
(C:\Users\Admin\Desktop\CLF_Practical_Exam\C\Users\HP)
4. Setupapi Log
(C:\Users\Admin\Desktop\CLF_Practical_Exam\C\Windows\INF)
5. Amcache Hive
(C:\Users\Admin\Desktop\CLF_Practical_Exam\C\Windows\AppCompat\Programs)

USB Detective v1.6.3 Community Edition (non-commercial use only) [002]

Serial/UID	Description	First Connected (UTC)	Last Connected (UTC)	Last Disconnected (UTC)	
4C530000150215104285	SanDisk Ultra USB Device	01-Jan-01 12:00:00 AM	21-Apr-23 5:16:23 AM	21-Apr-23 6:14:44 AM	A
4C530000300214115441	SanDisk Ultra USB Device	01-Jan-01 12:00:00 AM	18-Apr-23 9:59:25 AM	18-Apr-23 10:09:15 AM	P
458284BB210A	Sony Hard Drive USB Device	01-Jan-01 12:00:00 AM	19-Apr-23 6:18:03 AM	19-Apr-23 7:59:10 AM	E
04011c9a21e154fb8df920f5032cdc3f212985e45587efe1af1f8f6ec3849a0	USB SanDisk 3.2Gen1 USB Device	01-Jan-01 12:00:00 AM	13-Feb-23 7:01:40 AM	11-Jan-23 11:03:26 AM	
04011c9a21e154fb8df920f5032cdc3f212985e45587efe1af1f8f6ec3849a0d48cf00000000000000000c420eb1f000b7d188155810797acc8a3	SanDisk 3.2Gen1	01-Jan-01 12:00:00 AM		11-Jan-23 11:03:26 AM	
583420687e808000000	SK hynix BC711 HFMS12GD3JX013N	01-Jan-01 12:00:00 AM			
48dc792d4808040000	WDC WD10EZEX-60WN4A2	01-Jan-01 12:00:00 AM			
03025422082120195359	SANDISK CRUZER BLADE	01-Jan-01 12:00:00 AM			
C0AB2FE8	GENERIC FLASH DISK	01-Jan-01 12:00:00 AM			

26-Apr-23 11:08:34 AM UTC: Performing additional correlation across provided artifacts.
 26-Apr-23 11:08:34 AM UTC: Populating results grid and checking for duplicate timestamps.
 26-Apr-23 11:08:34 AM UTC: 9 devices were identified by USB Detective!
 26-Apr-23 11:08:34 AM UTC: Processing of DESKTOP-PR1FDQP is complete.
 26-Apr-23 11:08:36 AM UTC: 9 reported timestamps in the first connected column are identical! You may want to investigate this further.

Timestamp Consistency Levels
 Not Calculated Mid
 Low High

Final Answer:

	Description	
	SanDisk Ultra USB Device	
	SanDisk Ultra USB Device	
	Sony Hard Drive USB Device	
	USB SanDisk 3.2Gen1 USB Device	
3	SanDisk 3.2Gen1	
	SK hynix BC711 HFM512GD3JX013N	
	WDC WD10EZEX-60WN4A2	
	SANDISK CRUZER BLADE	
	GENERIC FLASH DISK	

(4) Identify the file having manipulated time stamp.

Tool Used:

MFT Explorer

File Used:

MFT File

MFT Explorer v2.0.0.0

File Tools Help

Name

C:\Users\Admin\Desktop\CLF_Pract

\$Extend
\$RECYCLE.BIN
CEH
DCM2
Forensics
MSIcd877.tmp
Recovery
System Volume Information

Properties

Copied ☒
Has ADS ☐
Is deleted ☐
Is directory ☐
Possible Timestamped ☒

Drag a column header here to group by that column

Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Created On	FN_Created On	SI_Modified On	FN_Modified On	SI_Last Accessed	FN_Last Accessed	SI_Record Char
No image data											
	System Volume Information	.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2022-10-22 00:...		2023-01-18 06:...	2022-10-22 00:5...	2023-04-24 03:49...	2022-10-22 00:53:...	2023-01-18
	~\$comment.docx	.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-04-24 05:...		2023-04-24 05:...		2023-04-24 05:57...		2023-04-24
	~\$WRL0001.tmp	.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-04-24 05:...		2023-04-24 05:...		2023-04-24 05:57...		2023-04-24
	\$AttrDef	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	\$BadClus	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	\$Bitmap	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	\$Boot	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	\$LogFile	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	\$MFT	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	\$MFTMirr	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	\$Secure	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	\$UpCase	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	\$Volume	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22
	document.docx	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-01-07 06:...	2023-04-24 05:5...	2017-07-10 13:...	2023-04-24 05:5...	2023-04-24 06:00...	2023-04-24 05:57:...	2023-04-24
	en_windows_10_multiple_editions_x64_dvd_6846432.iso	.	<input type="checkbox"/>	<input type="checkbox"/>	2023-02-02 10:...		2017-02-12 12:...	2023-02-02 10:5...	2023-04-18 10:08...	2023-02-02 10:59:...	2023-04-18
	SIPT-Workstation.ova	.	<input type="checkbox"/>	<input type="checkbox"/>	2023-01-17 11:...		2021-06-16 08:...	2023-01-17 11:0...	2023-01-17 11:04...	2023-01-17 11:02:...	2023-01-17

00000000 46 49 4C 45 30 00 03 00 76 80 00 E4 00 00 00 00
00000010 06 00 01 00 38 00 01 00 88 01 00 00 00 04 00 00
00000020 00 00 00 00 00 00 00 00 06 00 00 00 E9 2D 00 00
00000030 04 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00
00000040 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00
00000050 80 6C A1 2E 8E 03 D8 01 80 C4 B6 D0 7E F9 D2 01
00000060 40 CD F5 1D 72 76 D9 01 F3 71 AA 1E 72 76 D9 01
00000070 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080 00 00 00 00 11 01 00 00 00 00 00 00 00 00 00
00000090 88 46 86 00 00 00 00 00 30 00 00 00 78 00 00 00
000000A0 00 00 00 00 00 05 00 00 5C 00 00 00 18 00 01 00
000000B0 05 00 00 00 00 00 05 00 C4 A4 88 A0 71 76 D9 01
000000C0 08 FC 56 AC 71 76 D9 01 16 95 5D AC 71 76 D9 01

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Overview Details

[00002DE9-00000006, Entry-seq #: 0x2DE9-0x5, Offset: 0xB7A400, Flags: InUse, Log Sequence #: 0xE4008076, Mft Record To Base Record: Entry/seq: 0x0-0x0
Reference Count: 0x1, Fixup Data: Expected: 04-00 Fixup Actual: 00-00]00-00 (Fixup OK: True)

**** STANDARD INFO ****
Type: StandardInformation, Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x0, Content offset: 0x18, Resident: True
Flags: Archive, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x111, Quota Charged: 0x0
Update Sequence #: 0xB64688
Created On: 2022-01-07 06:17:01.0000000
Content Modified On: 2017-07-10 13:17:01.0000000
Record Modified On: 2023-04-24 06:00:48.5137728
Last Accessed On: 2023-04-24 06:00:49.6976371

**** FILE NAME ****
en_windows_10_multiple_editions_x64_dvd_6846432.iso

Data interpreter ?

Selected directory .

Directories 8 Files 15

Drag a column header here to group by that column

	Parent Path	Is Dir	Is Deleted	SI_Created On	FN_Created On	SI_Modified On	FN_Modified On	SI_Last Accessed	FN_Last Accessed	SI_Record Changed	FN_Record Changed	Timestamped	Copied
Y	0c			=	=	=	=	=	=	=	=		
	.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2022-10-22 00:...		2023-01-18 06:...	2022-10-22 00:5...	2023-04-24 03:49...	2022-10-22 00:53:...	2023-01-18 06:42:5...	2022-10-22 00:53:38...	<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-04-24 05:...		2023-04-24 05:...		2023-04-24 05:57...		2023-04-24 05:57:2...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-04-24 05:...		2023-04-24 05:...		2023-04-24 05:57...		2023-04-24 05:57:3...	2023-04-24 05:57:37...	<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...		<input type="checkbox"/>	<input type="checkbox"/>
	.	<input type="checkbox"/>	<input type="checkbox"/>	2022-10-22 08:...		2022-10-22 08:...		2022-10-22 08:49...		2022-10-22 08:49:4...			

(5) Following is the email header. Analyse the header and identify whether it is legitimate or not. If not, from where it was sent.

The Given Email is **Not Legitimate / Fake.**

Mon, 02 May 2022 03:08:51 -0700 (PDT)
Received-SPF: **softfail** (google.com: domain of transitioning tajvindersingh81@gmail.com does not designate 101.99.94.116 as permitted sender) client-ip=101.99.94.116;
Authentication-Results: mx.google.com;
spf=softfail (google.com: domain of transitioning tajvindersingh81@gmail.com does not designate 101.99.94.116 as permitted sender) smtp.mailfrom=tajvindersingh81@gmail.com;

dmARC=fail (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Received: by emkei.cz (Postfix, from userid 33) id 3AE2C18C532; Mon,
2 May 2022 12:08:25 +0200 (CEST)

- ✓ Email Evidence is in Email itself (Header)!
- ✓ Tracing -> Examination of an Email Header to determine its point of origin

Original Message

Message ID	<T2FGj9qC3WeJJ9VGtBiWCQ@notifications.google.com>
Created at:	Wed, Apr 19, 2023 at 10:18 AM (Delivered after 0 seconds)
From:	"Ami B Mehta TA2 SVNIT (Classroom)" <no-reply@classroom.google.com>
To:	u19cs012@coed.svnit.ac.in
Subject:	New assignment: "Assignment 6"
SPF:	PASS with IP 209.85.220.69 Learn more
DKIM:	'PASS' with domain google.com Learn more
DMARC:	'PASS' Learn more

[Download Original](#)

Ideally, It should pass all SPF, DKIM & DMARC.

Received: from **emkei.cz (emkei.cz. [101.99.94.116])**


by mx.google.com with ESMTPS id gj22-

20020a170907741600b006f38e90d86fsi11059076ejc.256.2022.05.02.03.08.51

for <thakarakash@gmail.com>

(version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);

Mon, 02 May 2022 03:08:51 -0700 (PDT)

Search

MY IP

IP LOOKUP

HIDE MY IP

VPNS ▾

IP Details For: 101.99.94.116

Decimal: 1701011060

Hostname: emkei.cz

ASN: 45839

ISP: Shinjiru Technology Sdn Bhd

Services: Datacenter

Assignment: [Likely Static IP](#)


Country: Malaysia

State/Region: Wilayah Persekutuan Kuala Lumpur

City: Kuala Lumpur

Latitude: 3.1413 (3° 8' 28.68" N)

Longitude: 101.6866 (101° 41' 11.84" E)



CLICK TO CHECK BLACKLIST STATUS

Sent Location:

Country:Malaysia

State/Region:Wilayah Persekutuan Kuala Lumpur

City:Kuala Lumpur

Latitude:3.1413 (3° 8' 28.68" N)

Longitude:101.6866 (101° 41' 11.84" E)

SUBMITTED BY:

U19CS012

BHAGYA VINOD RANA