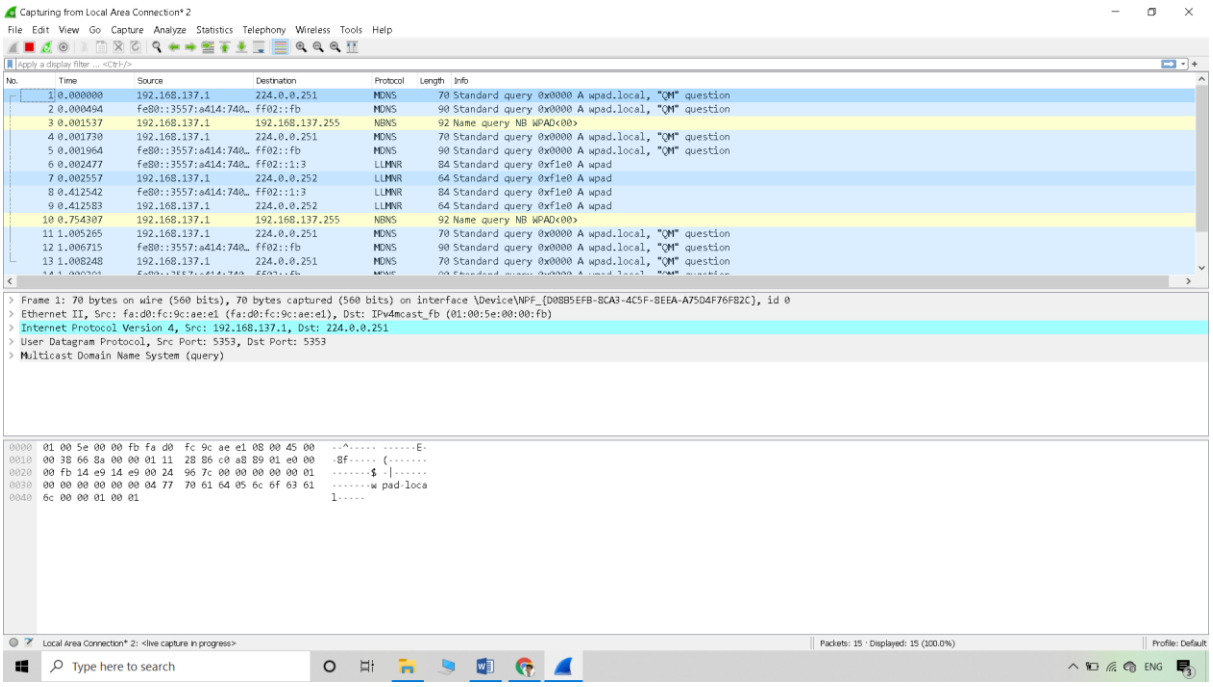
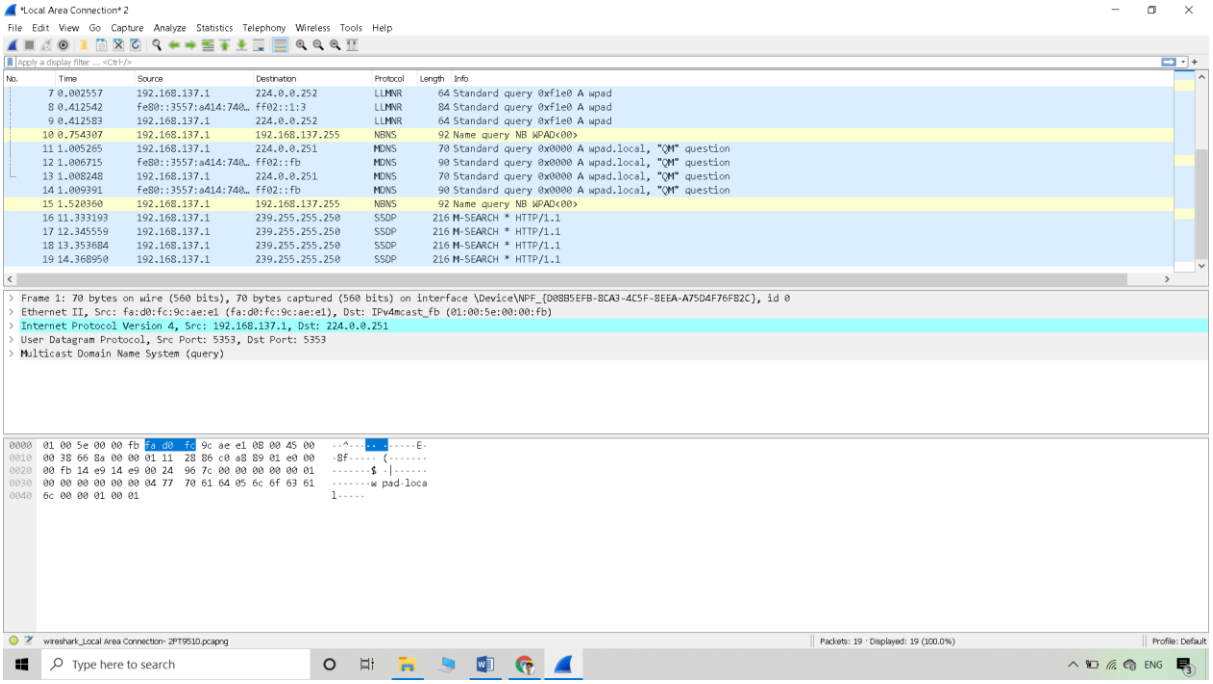
Practical 1

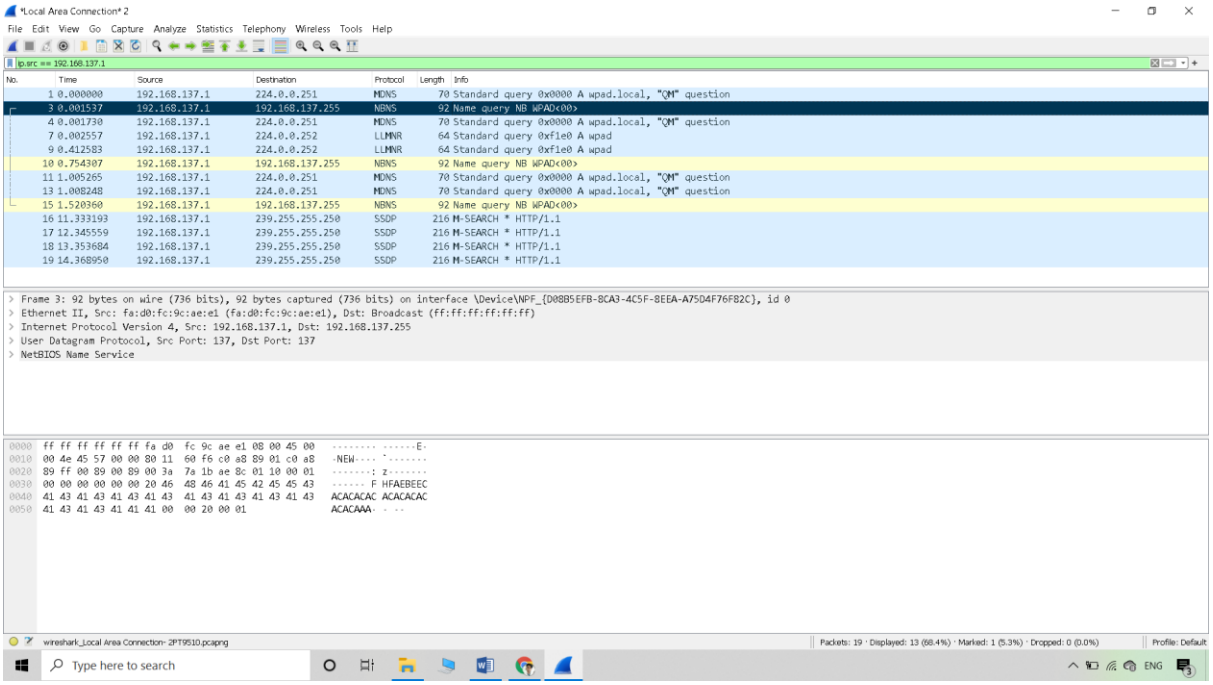
Aim : Capturing and analysing network packets using wireshark.

- Identification the live network
- Capture packets
- Analze the captured packets

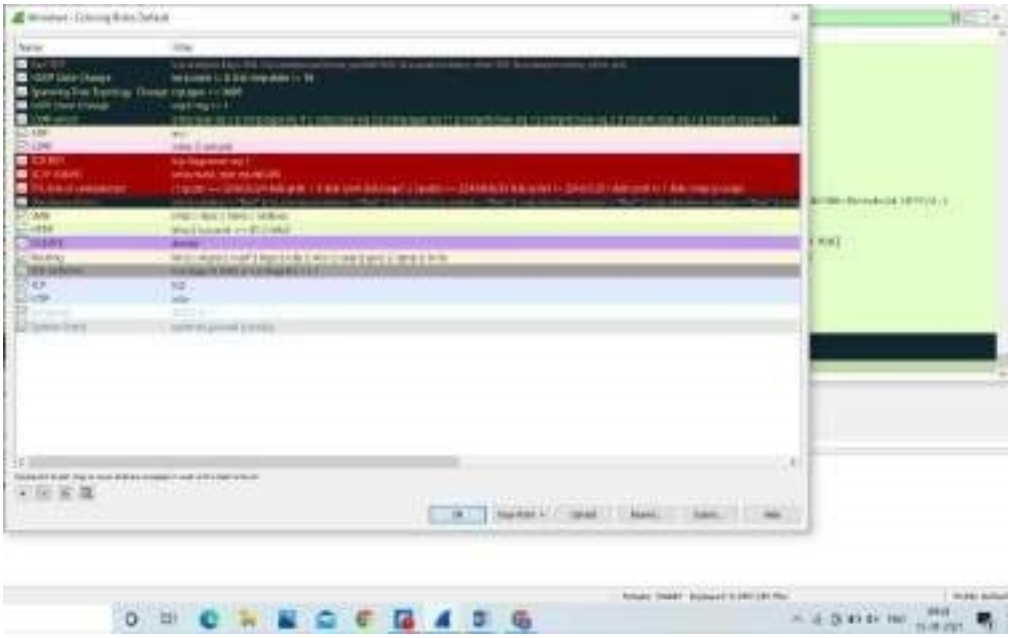


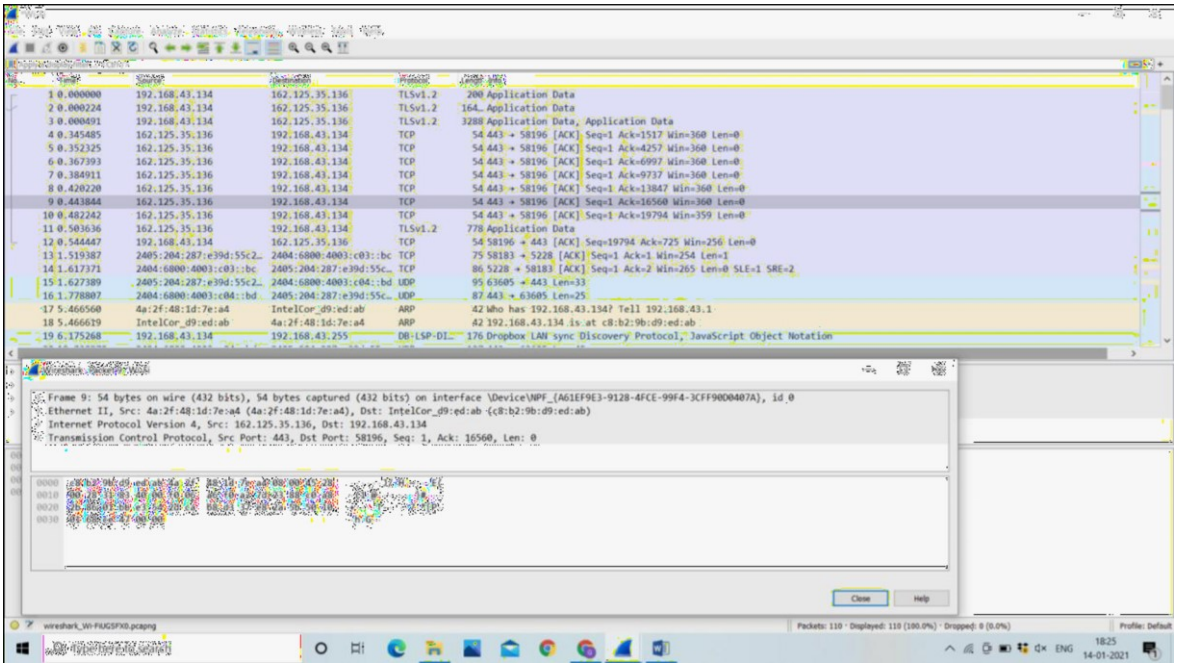
Analyse the captured packets

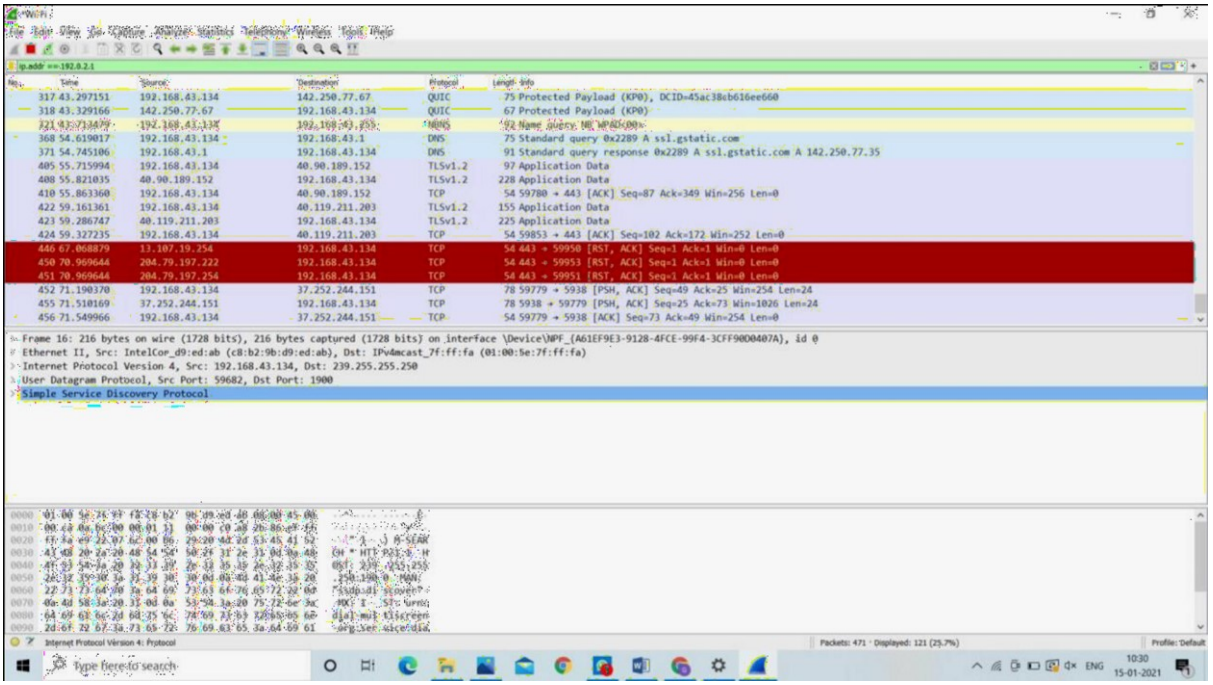




Display all the filters




1 0.000000 192.168.43.134 162.125.35.136 TLSv1.2 200 Application Data
2 0.000224 192.168.43.134 162.125.35.136 TLSv1.2 164… Application Data
3 0.000491 192.168.43.134 162.125.35.136 TLSv1.2 3288 Application Data, Application Data
4 0.345485 162.125.35.136 192.168.43.134 TCP 54 443 → 58196 [ACK] Seq=1 Ack=1517 Win=360 Len=0
5 0.352325 162.125.35.136 192.168.43.134 TCP 54 443 → 58196 [ACK] Seq=1 Ack=4257 Win=360 Len=0
6 0.367393 162.125.35.136 192.168.43.134 TCP 54 443 → 58196 [ACK] Seq=1 Ack=6997 Win=360 Len=0
7 0.384911 162.125.35.136 192.168.43.134 TCP 54 443 → 58196 [ACK] Seq=1 Ack=9737 Win=360 Len=0
8 0.420220 162.125.35.136 192.168.43.134 TCP 54 443 → 58196 [ACK] Seq=1 Ack=13847 Win=360 Len=0
9 0.443844 162.125.35.136 192.168.43.134 TCP 54 443 → 58196 [ACK] Seq=1 Ack=16560 Win=360 Len=0
10 0.482242 162.125.35.136 192.168.43.134 TCP 54 443 → 58196 [ACK] Seq=1 Ack=19794 Win=359 Len=0
11 0.503636 162.125.35.136 192.168.43.134 TLSv1.2 778 Application Data
12 0.544447 192.168.43.134 162.125.35.136 TCP 54 58196 → 443 [ACK] Seq=19794 Ack=725 Win=256 Len=0
13 1.519387 2405:204:287:e39d:55c2… 2404:6800:4003:c03::bc TCP 75 58183 → 5228 [ACK] Seq=1 Ack=1 Win=254 Len=1
14 1.617371 2404:6800:4003:c03::bc 2405:204:287:e39d:55c… TCP 86 5228 → 58183 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
15 1.627389 2405:204:287:e39d:55c2… 2404:6800:4003:c04::bd UDP 95 63605 → 443 Len=33
16 1.778807 2404:6800:4003:c04::bd 2405:204:287:e39d:55c… UDP 87 443 → 63605 Len=25
17 5.466560 4a:2f:48:1d:7e:a4 IntelCor_d9:ed:ab ARP 42 Who has 192.168.43.134? Tell 192.168.43.1
18 5.466619 IntelCor_d9:ed:ab 4a:2f:48:1d:7e:a4 ARP 42 192.168.43.134 is at c8:b2:9b:d9:ed:ab
19 6.175268 192.168.43.134 192.168.43.255 DB-LSP-DI… 176 Dropbox LAN sync Discovery Protocol, JavaScript Object Notation
Frame 9: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{A61EF9E3-9128-4FCE-99F4-3CFF90D0407A}, id 0
Ethernet II, Src: 4a:2f:48:1d:7e:a4 (4a:2f:48:1d:7e:a4), Dst: IntelCor_d9:ed:ab (c8:b2:9b:d9:ed:ab)
Internet Protocol Version 4, Src: 162.125.35.136, Dst: 192.168.43.134
Transmission Control Protocol, Src Port: 443, Dst Port: 58196, Seq: 1, Ack: 16560, Len: 0
Close
Help
Packets: 110 · Displayed: 110 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
ENG
1825
14-01-2021

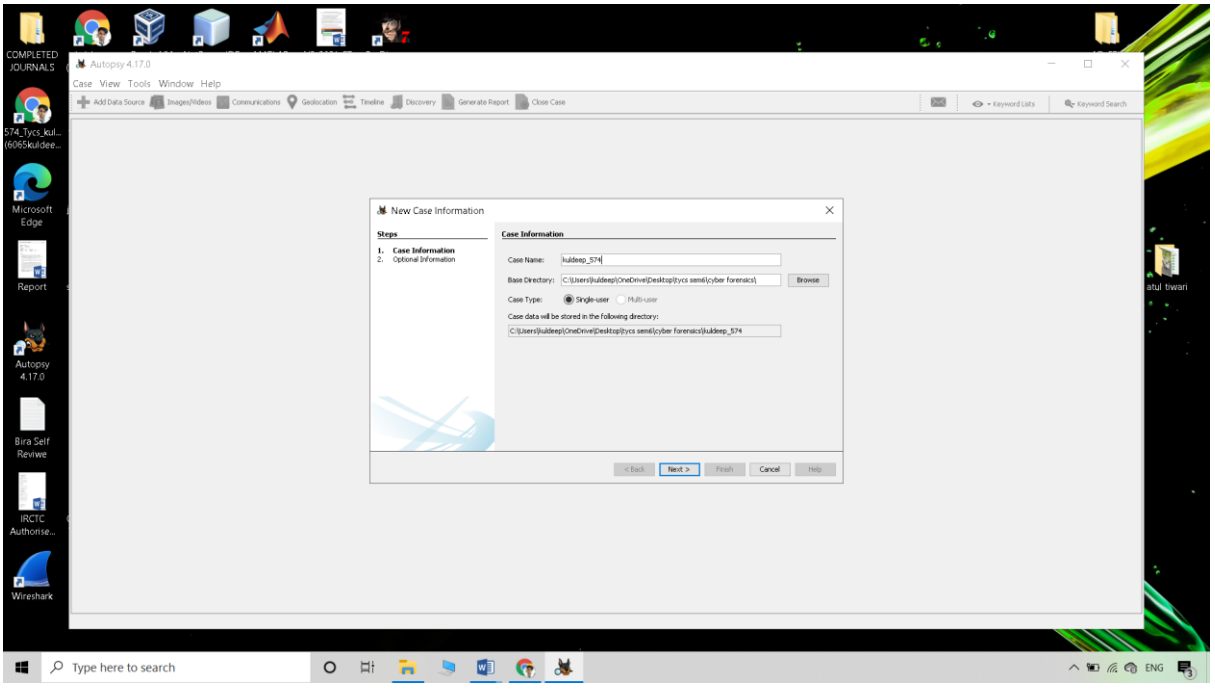

Wi-Fi
ip.addr == 192.0.2.1
No. Time Source Destination Protocol Length Info
317 43.297151 192.168.43.134 142.250.77.67 QUIC 75 Protected Payload (KP0), DCID=45ac38cb616ee660
318 43.329166 142.250.77.67 192.168.43.134 QUIC 67 Protected Payload (KP0)
368 54.619017 192.168.43.134 192.168.43.1 DNS 75 Standard query 0x2289 A ssl.gstatic.com
371 54.745106 192.168.43.1 192.168.43.134 DNS 91 Standard query response 0x2289 A ssl.gstatic.com A 142.250.77.35
405 55.715994 192.168.43.134 40.90.189.152 TLSv1.2 97 Application Data
408 55.821035 40.90.189.152 192.168.43.134 TLSv1.2 228 Application Data
410 55.863360 192.168.43.134 40.90.189.152 TCP 54 59780 → 443 [ACK] Seq=87 Ack=349 Win=256 Len=0
422 59.161361 192.168.43.134 40.119.211.203 TLSv1.2 155 Application Data
423 59.286747 40.119.211.203 192.168.43.134 TLSv1.2 225 Application Data
424 59.327235 192.168.43.134 40.119.211.203 TCP 54 59853 → 443 [ACK] Seq=102 Ack=172 Win=252 Len=0
446 67.068879 13.107.19.254 192.168.43.134 TCP 54 443 → 59950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
450 70.969644 204.79.197.222 192.168.43.134 TCP 54 443 → 59953 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
451 70.969644 204.79.197.254 192.168.43.134 TCP 54 443 → 59951 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
452 71.190370 192.168.43.134 37.252.244.151 TCP 78 59779 → 5938 [PSH, ACK] Seq=49 Ack=25 Win=254 Len=24
455 71.510169 37.252.244.151 192.168.43.134 TCP 78 5938 → 59779 [PSH, ACK] Seq=25 Ack=73 Win=1026 Len=24
456 71.549966 192.168.43.134 37.252.244.151 TCP 54 59779 → 5938 [ACK] Seq=73 Ack=49 Win=254 Len=0
Frame 16: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_{A61EF9E3-9128-4FCE-99F4-3CFF9000407A}, id 0
Ethernet II, Src: IntelCor_d9:ed:ab (c8:b2:9b:d9:ed:ab), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.43.134, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 59682, Dst Port: 1900
Simple Service Discovery Protocol
Internet Protocol Version 4: Protocol
Packets: 471 · Displayed: 121 (25.7%)
Profile: Default
Type here to search
ENG
10:30
15-01-2021

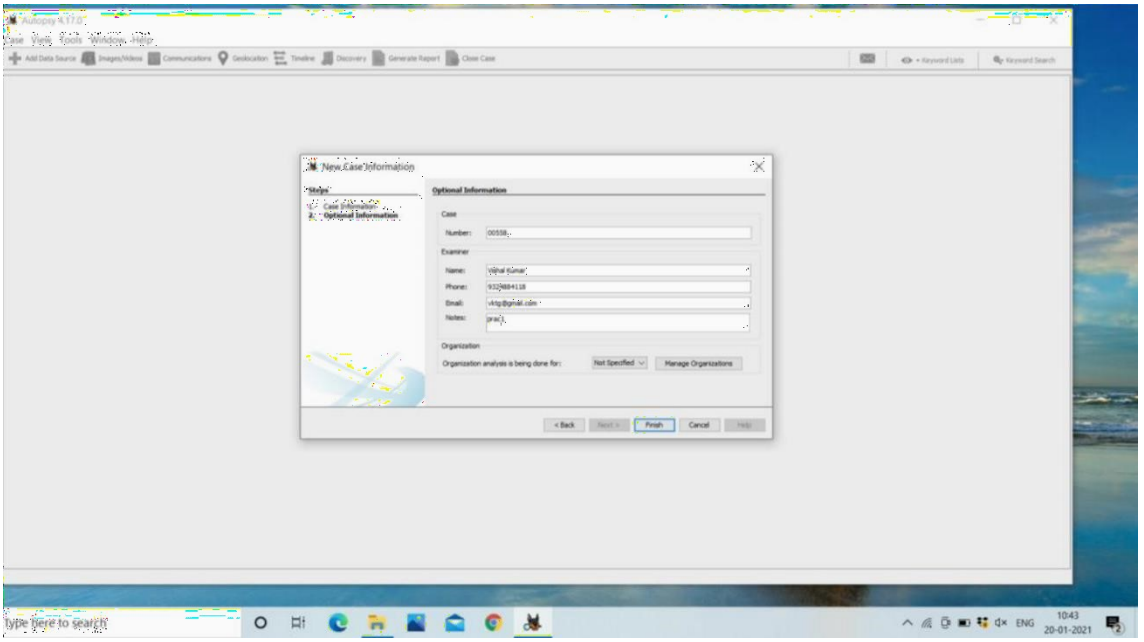
Practical 2

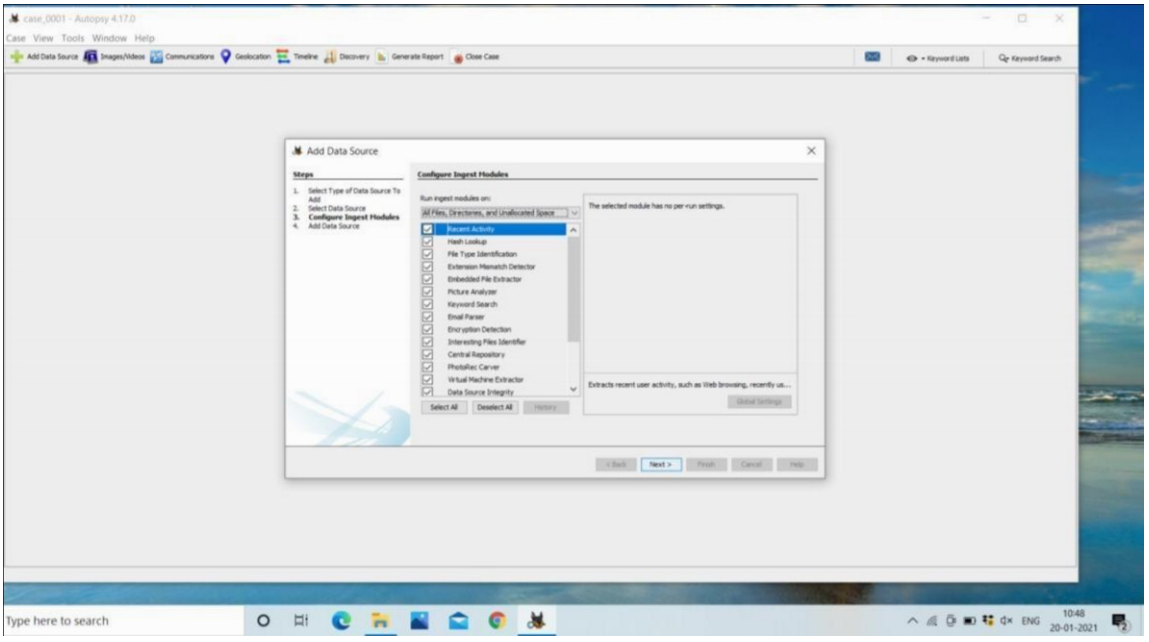
AIM :- Forensics Case Study : Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy .

Step 1 : Open Autopsy

Step 2 : Click on new case



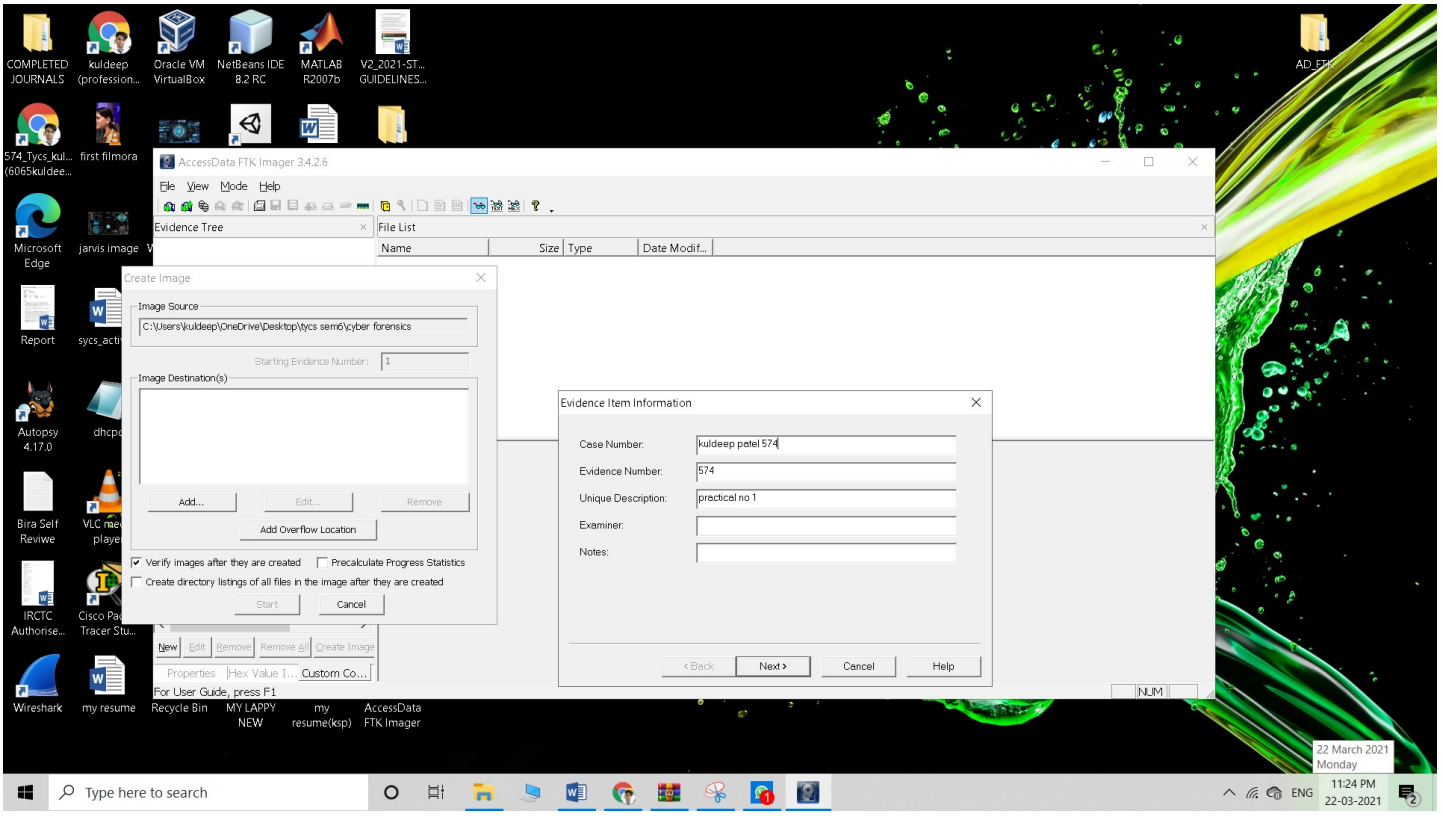

New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number:
Examiner
Name:
Phone:
Email:
Notes:
Organization
Organization analysis is being done for:
Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help
Type here to search
ENG
10:43
20-01-2021

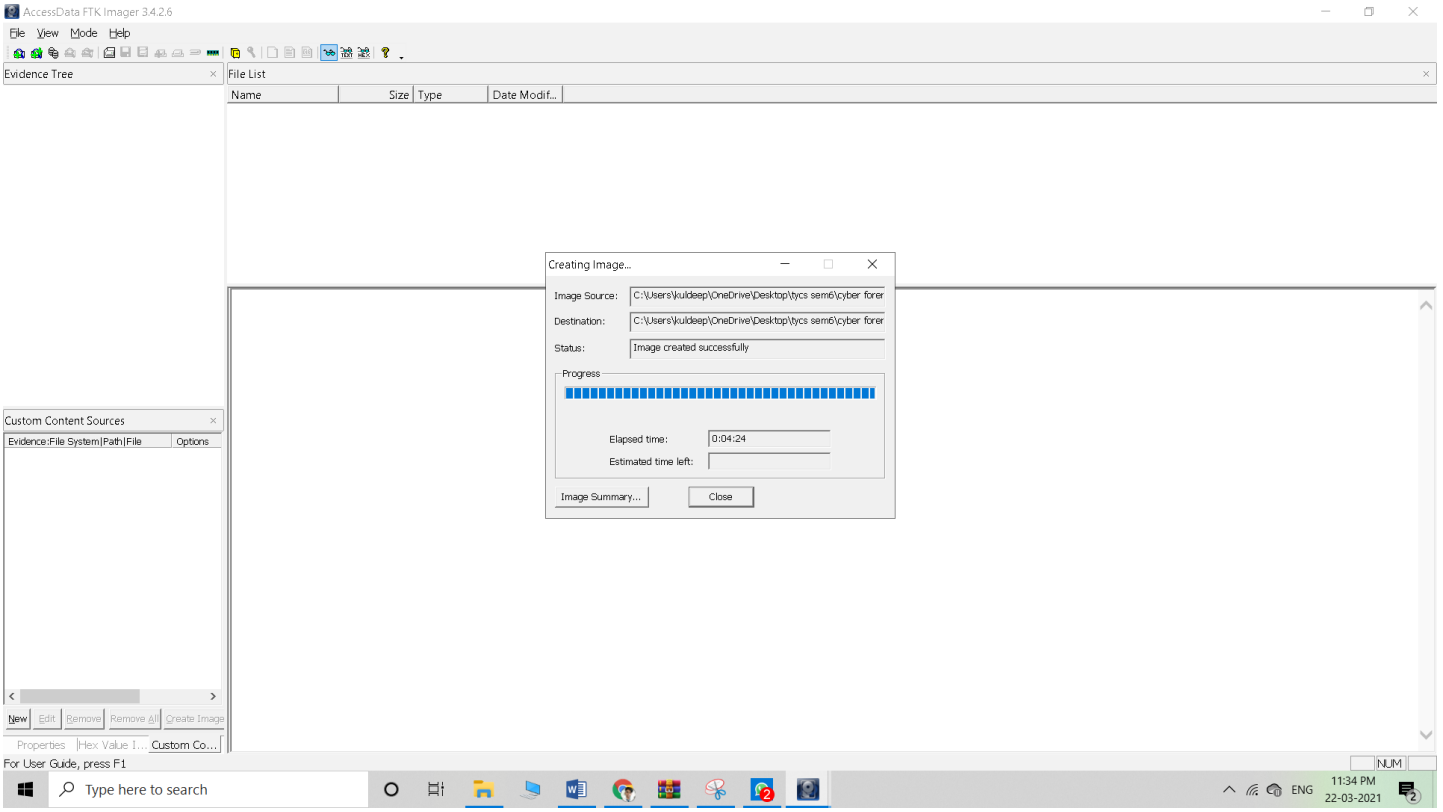

case_0001 - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Configure Ingest Modules
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, recently us...
Global Settings
Select All
Deselect All
History
< Back
Next >
Finish
Cancel
Help
Type here to search
ENG
10:48
20-01-2021

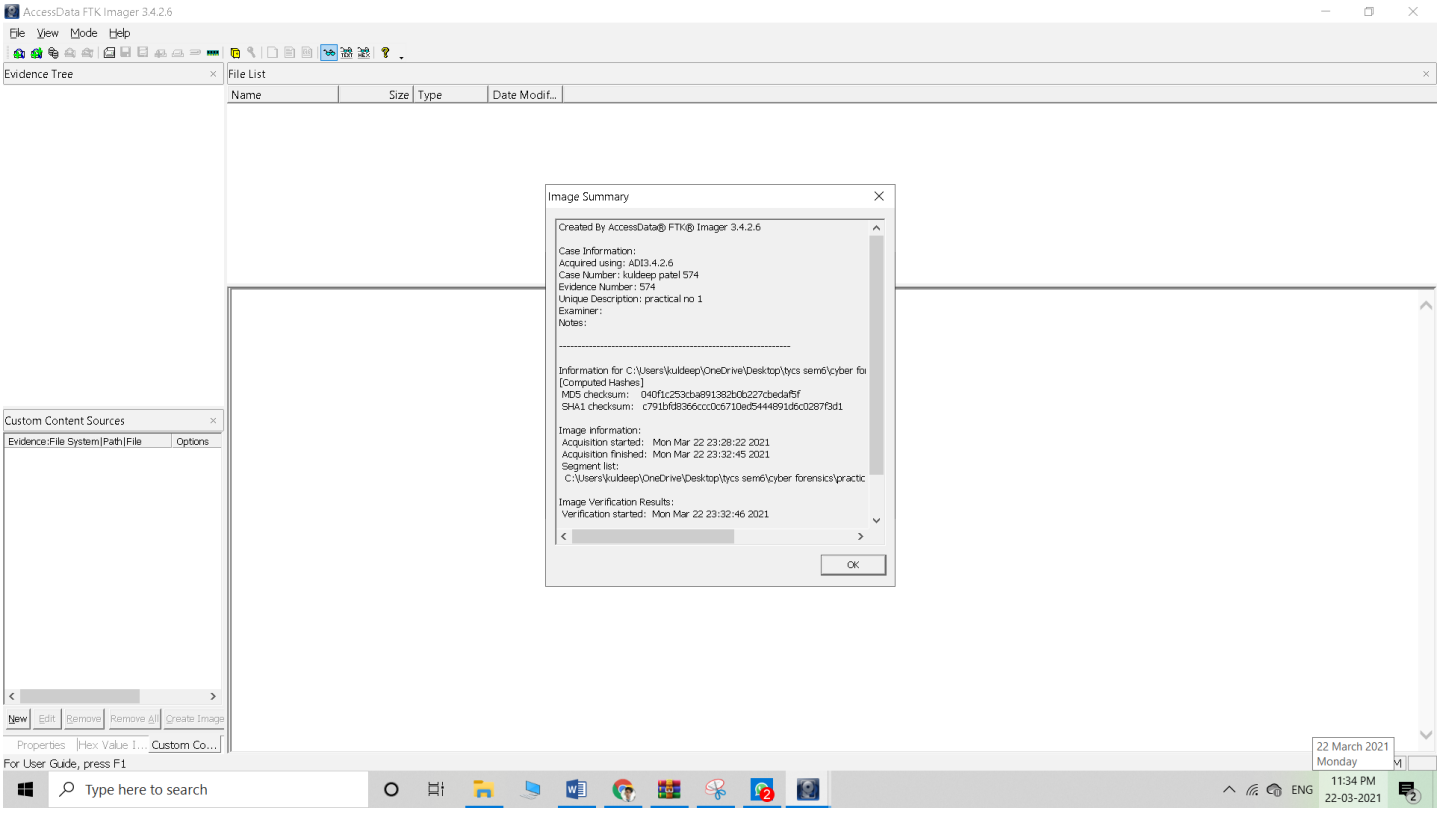
Practical no 3

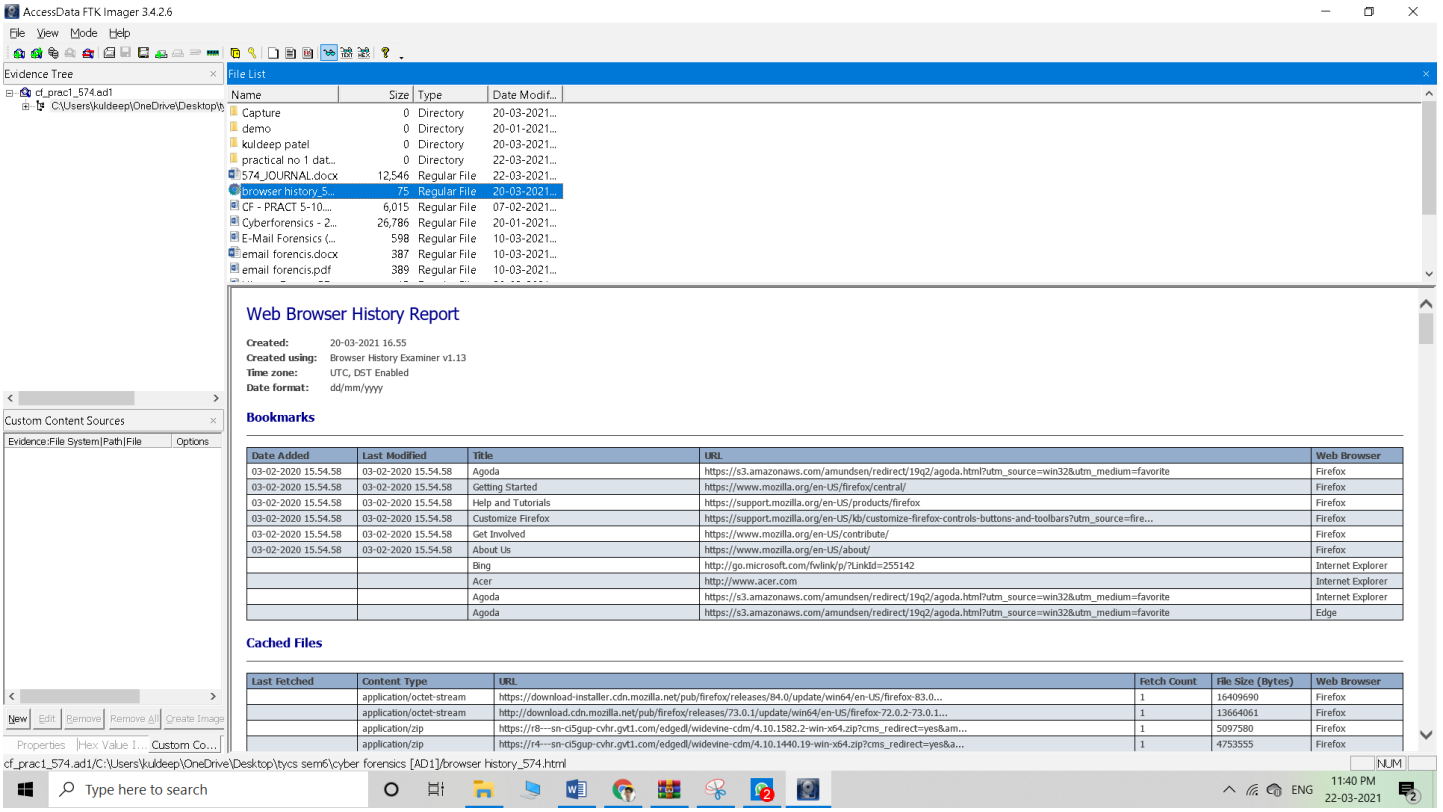
Aim : Creating a Forensic Image using FTK Imager/Encase Imager :

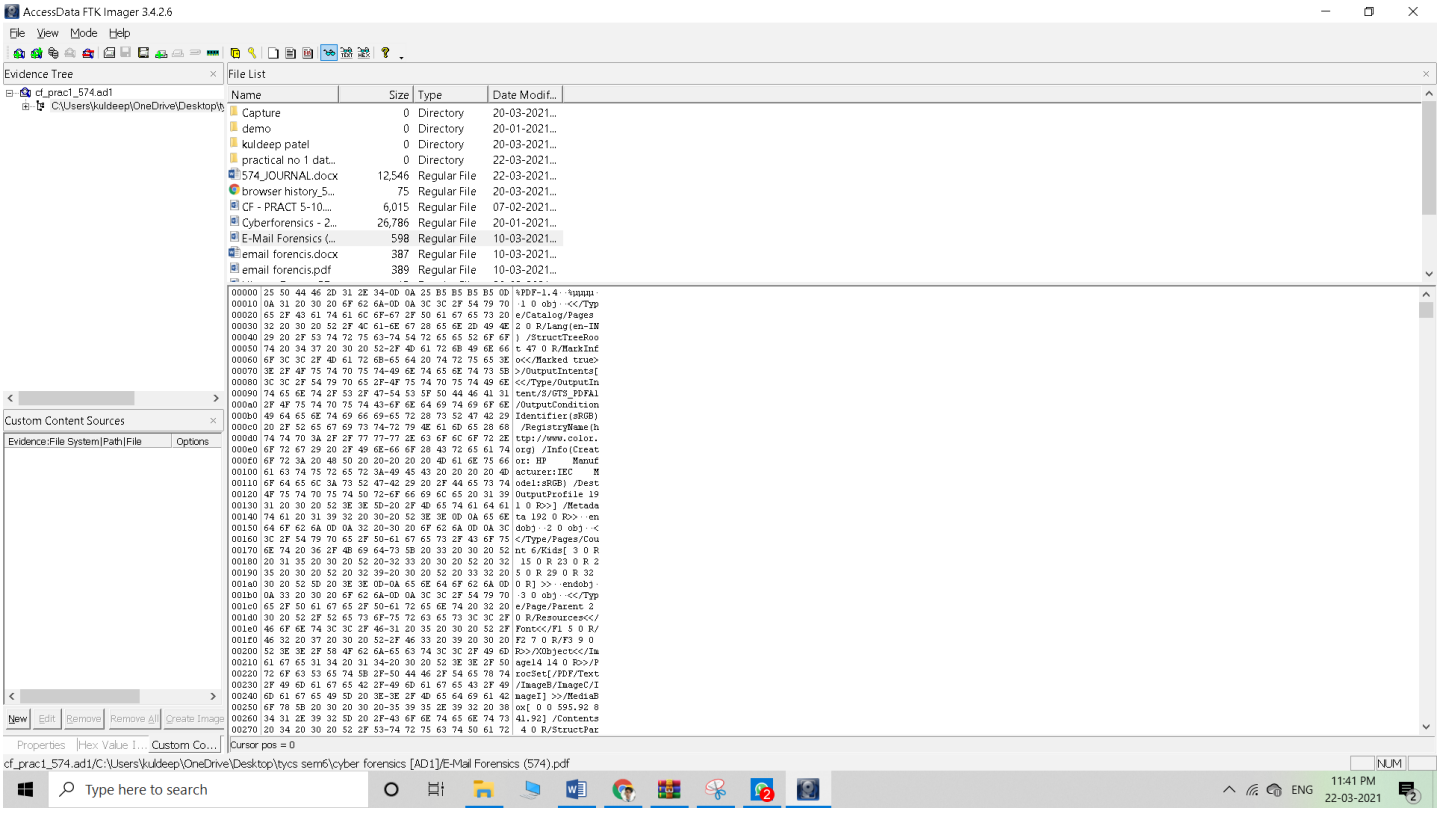
- Creating Forensic Image
- Check Integrity of Data
- Analyse Forensic Image

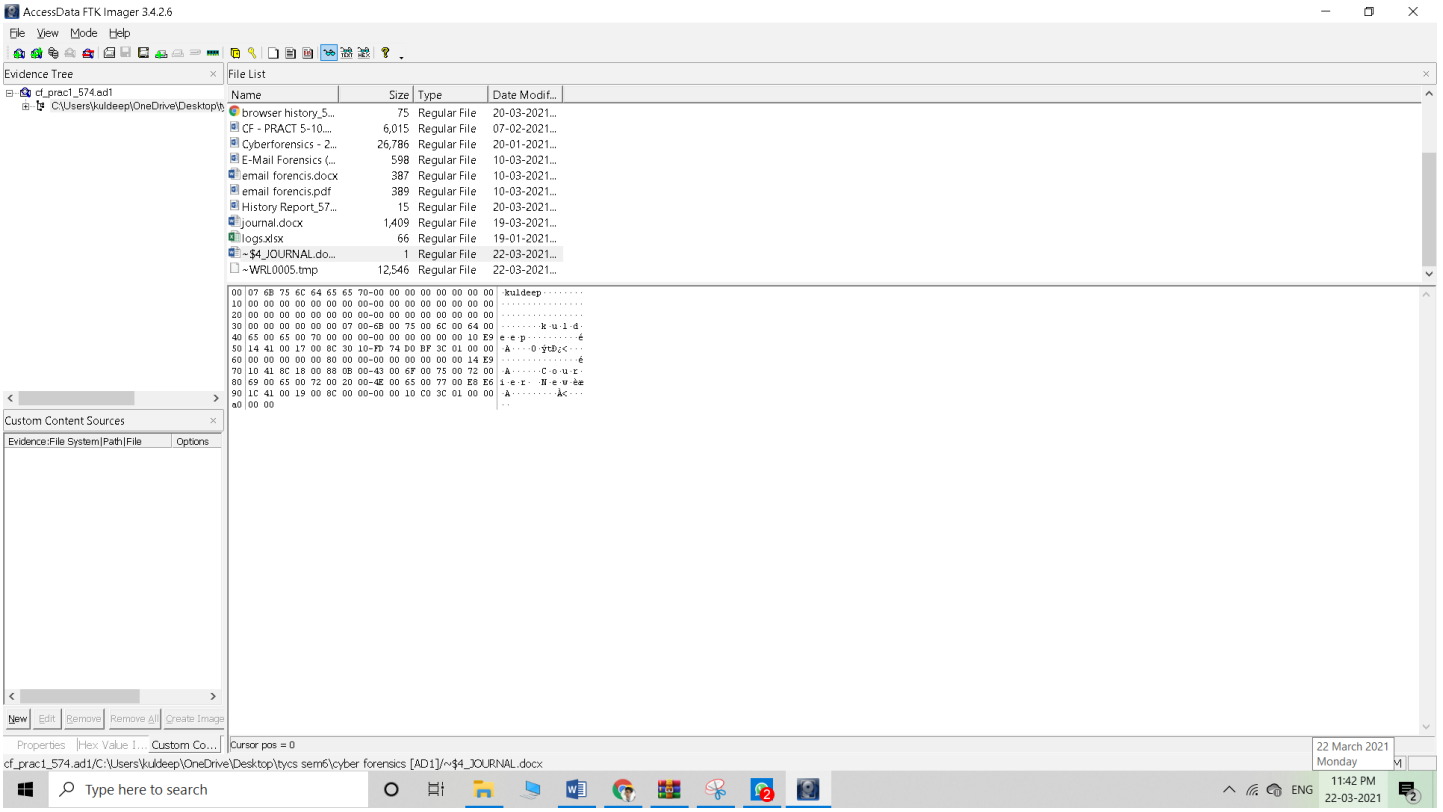


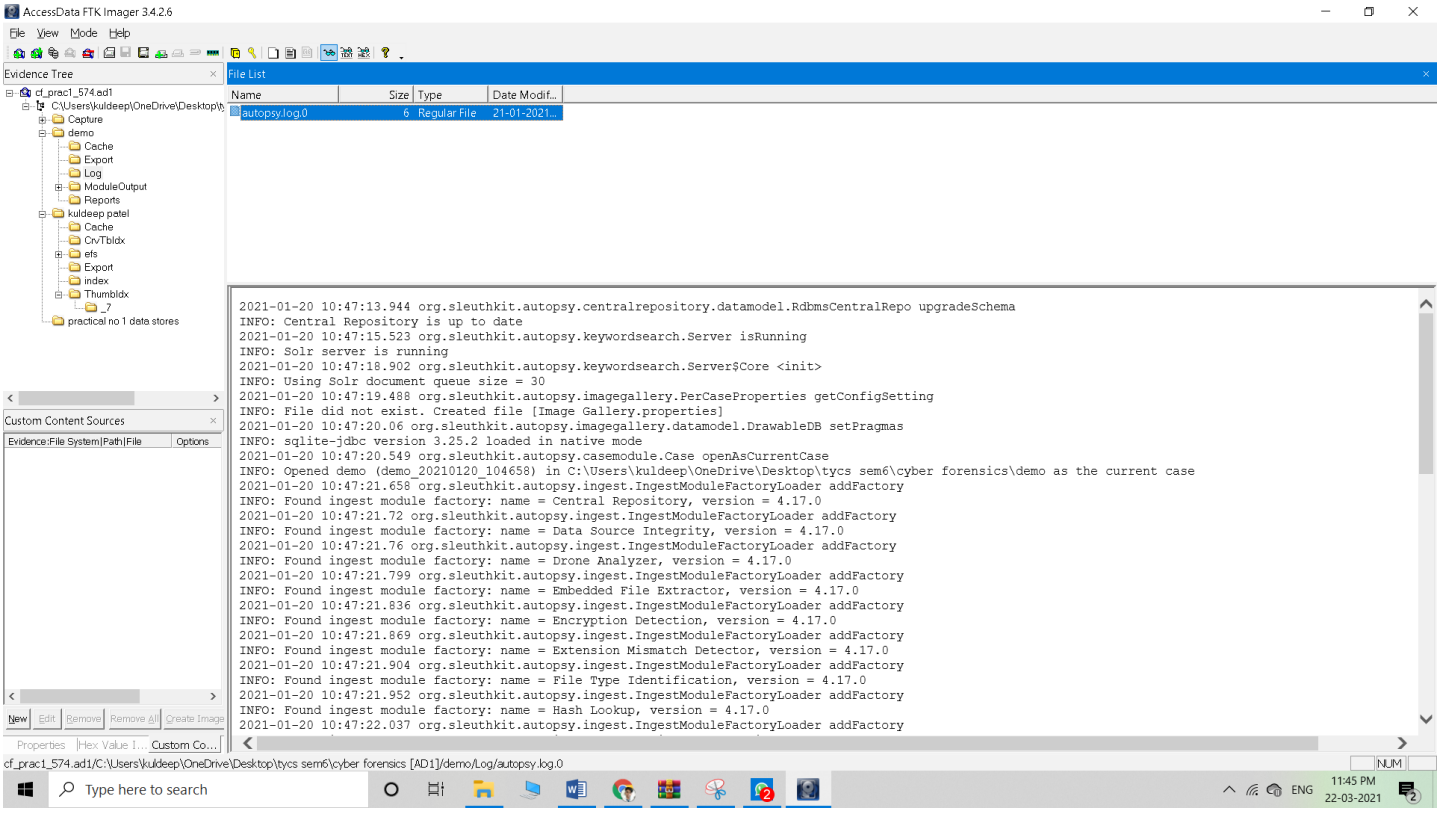

AccessData FTK Imager 3.4.2.6
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modif...
Creating Image...
Image Source: C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forer
Destination: C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forer
Status: Image created successfully
Progress
Elapsed time: 0:04:24
Estimated time left:
Image Summary... Close
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value I... Custom Co...
For User Guide, press F1
NUM
Type here to search
ENG 11:34 PM 22-03-2021


AccessData FTK Imager 3.4.2.6
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modif...
Image Summary
Created By AccessData® FTK® Imager 3.4.2.6
Case Information:
Acquired using: ADI3.4.2.6
Case Number: kuldeep patel 574
Evidence Number: 574
Unique Description: practical no 1
Examiner:
Notes:
Information for C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber fo
[Computed Hashes]
MD5 checksum: 040f1c253cba891382b0b227cbedaf5f
SHA1 checksum: c791bfd8366ccc0c6710ed5444891d6c0287f3d1
Image information:
Acquisition started: Mon Mar 22 23:28:22 2021
Acquisition finished: Mon Mar 22 23:32:45 2021
Segment list:
C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics\practic
Image Verification Results:
Verification started: Mon Mar 22 23:32:46 2021
OK
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value I... Custom Co...
For User Guide, press F1
22 March 2021 Monday
Type here to search
ENG 11:34 PM 22-03-2021


AccessData FTK Imager 3.4.2.6
File View Mode Help
Evidence Tree
cf_prac1_574.ad1
C:\Users\kuldeep\OneDrive\Desktop\t
File List
Name Size Type Date Modif...
Capture 0 Directory 20-03-2021...
demo 0 Directory 20-01-2021...
kuldeep patel 0 Directory 20-03-2021...
practical no 1 dat... 0 Directory 22-03-2021...
574_JOURNAL.docx 12,546 Regular File 22-03-2021...
browser history_5... 75 Regular File 20-03-2021...
CF - PRACT 5-10.... 6,015 Regular File 07-02-2021...
Cyberforensics - 2... 26,786 Regular File 20-01-2021...
E-Mail Forensics (... 598 Regular File 10-03-2021...
email forencis.docx 387 Regular File 10-03-2021...
email forencis.pdf 389 Regular File 10-03-2021...
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value I... Custom Co...
Web Browser History Report
Created: 20-03-2021 16.55
Created using: Browser History Examiner v1.13
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy
Bookmarks
Date Added | Last Modified | Title | URL | Web Browser
03-02-2020 15.54.58 | 03-02-2020 15.54.58 | Agoda | https://s3.amazonaws.com/amundsen/redirect/19q2/agoda.html?utm_source=win32&utm_medium=favorite | Firefox
03-02-2020 15.54.58 | 03-02-2020 15.54.58 | Getting Started | https://www.mozilla.org/en-US/firefox/central/ | Firefox
03-02-2020 15.54.58 | 03-02-2020 15.54.58 | Help and Tutorials | https://support.mozilla.org/en-US/products/firefox | Firefox
03-02-2020 15.54.58 | 03-02-2020 15.54.58 | Customize Firefox | https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=fire... | Firefox
03-02-2020 15.54.58 | 03-02-2020 15.54.58 | Get Involved | https://www.mozilla.org/en-US/contribute/ | Firefox
03-02-2020 15.54.58 | 03-02-2020 15.54.58 | About Us | https://www.mozilla.org/en-US/about/ | Firefox
Bing | http://go.microsoft.com/fwlink/p/?LinkId=255142 | Internet Explorer
Acer | http://www.acer.com | Internet Explorer
Agoda | https://s3.amazonaws.com/amundsen/redirect/19q2/agoda.html?utm_source=win32&utm_medium=favorite | Internet Explorer
Agoda | https://s3.amazonaws.com/amundsen/redirect/19q2/agoda.html?utm_source=win32&utm_medium=favorite | Edge
Cached Files
Last Fetched | Content Type | URL | Fetch Count | File Size (Bytes) | Web Browser
application/octet-stream | https://download-installer.cdn.mozilla.net/pub/firefox/releases/84.0/update/win64/en-US/firefox-83.0... | 1 | 16409690 | Firefox
application/octet-stream | http://download.cdn.mozilla.net/pub/firefox/releases/73.0.1/update/win64/en-US/firefox-72.0.2-73.0.1... | 1 | 13664061 | Firefox
application/zip | https://r8---sn-ci5gup-cvhr.gvt1.com/edgedl/widevine-cdm/4.10.1582.2-win-x64.zip?cms_redirect=yes&am... | 1 | 5097580 | Firefox
application/zip | https://r4---sn-ci5gup-cvhr.gvt1.com/edgedl/widevine-cdm/4.10.1440.19-win-x64.zip?cms_redirect=yes&a... | 1 | 4753555 | Firefox
cf_prac1_574.ad1/C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics [AD1]/browser history_574.html
NUM
Type here to search
ENG 11:40 PM 22-03-2021


AccessData FTK Imager 3.4.2.6
File View Mode Help
Evidence Tree
cf_prac1_574.ad1
C:\Users\kuldeep\OneDrive\Desktop\t
File List
Name Size Type Date Modif...
Capture 0 Directory 20-03-2021...
demo 0 Directory 20-01-2021...
kuldeep patel 0 Directory 20-03-2021...
practical no 1 dat... 0 Directory 22-03-2021...
574_JOURNAL.docx 12,546 Regular File 22-03-2021...
browser history_5... 75 Regular File 20-03-2021...
CF - PRACT 5-10.... 6,015 Regular File 07-02-2021...
Cyberforensics - 2... 26,786 Regular File 20-01-2021...
E-Mail Forensics (... 598 Regular File 10-03-2021...
email forencis.docx 387 Regular File 10-03-2021...
email forencis.pdf 389 Regular File 10-03-2021...
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value I... Custom Co...
Cursor pos = 0
cf_prac1_574.ad1/C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics [AD1]/E-Mail Forensics (574).pdf
NUM
Type here to search
ENG 11:41 PM 22-03-2021

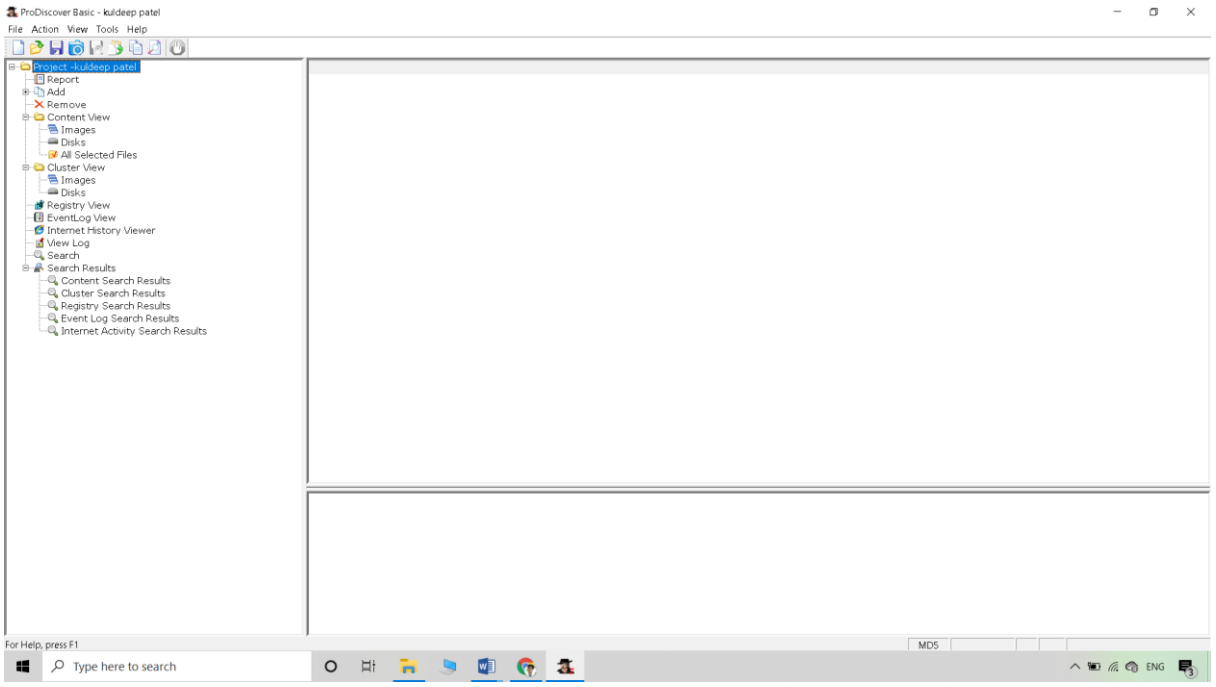

AccessData FTK Imager 3.4.2.6
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modif...
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value I... Custom Co...
Cursor pos = 0
cf_prac1_574.ad1/C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics [AD1]/~$4_JOURNAL.docx
Type here to search
ENG
11:42 PM
22-03-2021

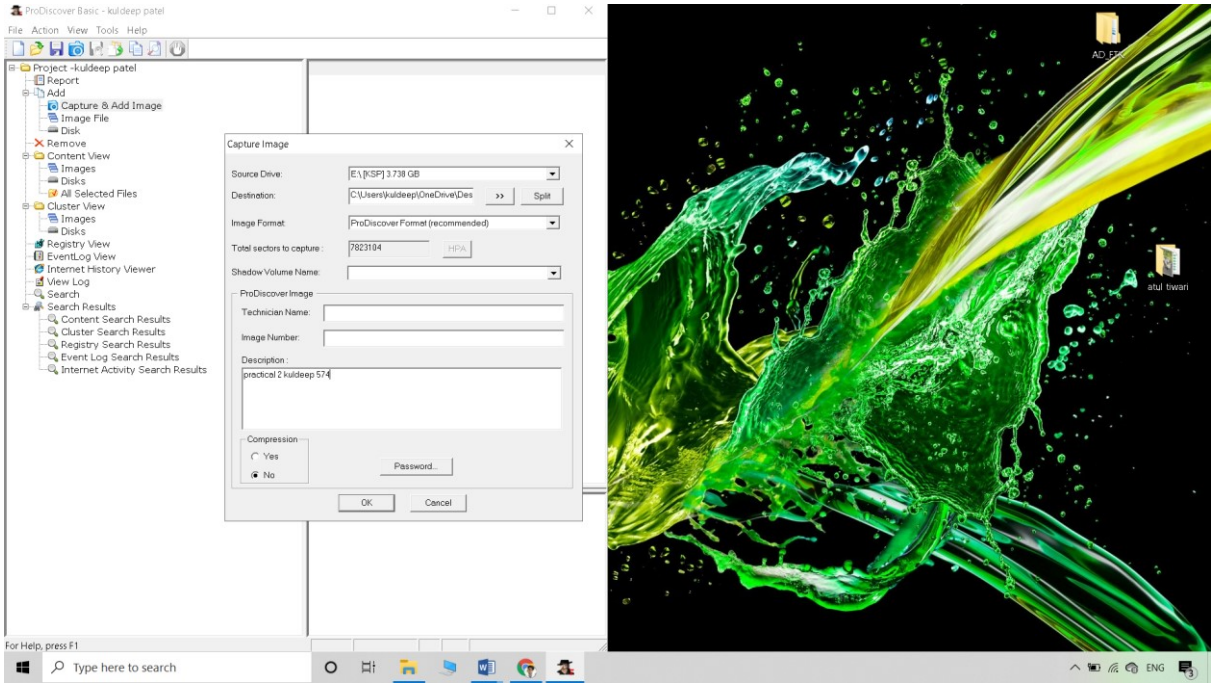

AccessData FTK Imager 3.4.2.6
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modif...
autopsy.log.0 6 Regular File 21-01-2021...
Capture
demo
Cache
Export
Log
ModuleOutput
Reports
kuldeep patel
Cache
CrvTbldx
efs
Export
index
Thumbldx
_7
practical no 1 data stores
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value I... Custom Co...
2021-01-20 10:47:13.944 org.sleuthkit.autopsy.centralrepository.datamodel.RdbmsCentralRepo upgradeSchema
INFO: Central Repository is up to date
2021-01-20 10:47:15.523 org.sleuthkit.autopsy.keywordsearch.Server isRunning
INFO: Solr server is running
2021-01-20 10:47:18.902 org.sleuthkit.autopsy.keywordsearch.Server$Core <init>
INFO: Using Solr document queue size = 30
2021-01-20 10:47:19.488 org.sleuthkit.autopsy.imagegallery.PerCaseProperties getConfigSetting
INFO: File did not exist. Created file [Image Gallery.properties]
2021-01-20 10:47:20.06 org.sleuthkit.autopsy.imagegallery.datamodel.DrawableDB setPragmas
INFO: sqlite-jdbc version 3.25.2 loaded in native mode
2021-01-20 10:47:20.549 org.sleuthkit.autopsy.casemodule.Case openAsCurrentCase
INFO: Opened demo (demo_20210120_104658) in C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics\demo as the current case
2021-01-20 10:47:21.658 org.sleuthkit.autopsy.ingest.IngestModuleFactoryLoader addFactory
INFO: Found ingest module factory: name = Central Repository, version = 4.17.0
2021-01-20 10:47:21.72 org.sleuthkit.autopsy.ingest.IngestModuleFactoryLoader addFactory
INFO: Found ingest module factory: name = Data Source Integrity, version = 4.17.0
2021-01-20 10:47:21.76 org.sleuthkit.autopsy.ingest.IngestModuleFactoryLoader addFactory
INFO: Found ingest module factory: name = Drone Analyzer, version = 4.17.0
2021-01-20 10:47:21.799 org.sleuthkit.autopsy.ingest.IngestModuleFactoryLoader addFactory
INFO: Found ingest module factory: name = Embedded File Extractor, version = 4.17.0
2021-01-20 10:47:21.836 org.sleuthkit.autopsy.ingest.IngestModuleFactoryLoader addFactory
INFO: Found ingest module factory: name = Encryption Detection, version = 4.17.0
2021-01-20 10:47:21.869 org.sleuthkit.autopsy.ingest.IngestModuleFactoryLoader addFactory
INFO: Found ingest module factory: name = Extension Mismatch Detector, version = 4.17.0
2021-01-20 10:47:21.904 org.sleuthkit.autopsy.ingest.IngestModuleFactoryLoader addFactory
INFO: Found ingest module factory: name = File Type Identification, version = 4.17.0
2021-01-20 10:47:21.952 org.sleuthkit.autopsy.ingest.IngestModuleFactoryLoader addFactory
INFO: Found ingest module factory: name = Hash Lookup, version = 4.17.0
2021-01-20 10:47:22.037 org.sleuthkit.autopsy.ingest.IngestModuleFactoryLoader addFactory
cf_prac1_574.ad1/C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics [AD1]/demo/Log/autopsy.log.0
NUM
Type here to search
ENG
11:45 PM
22-03-2021

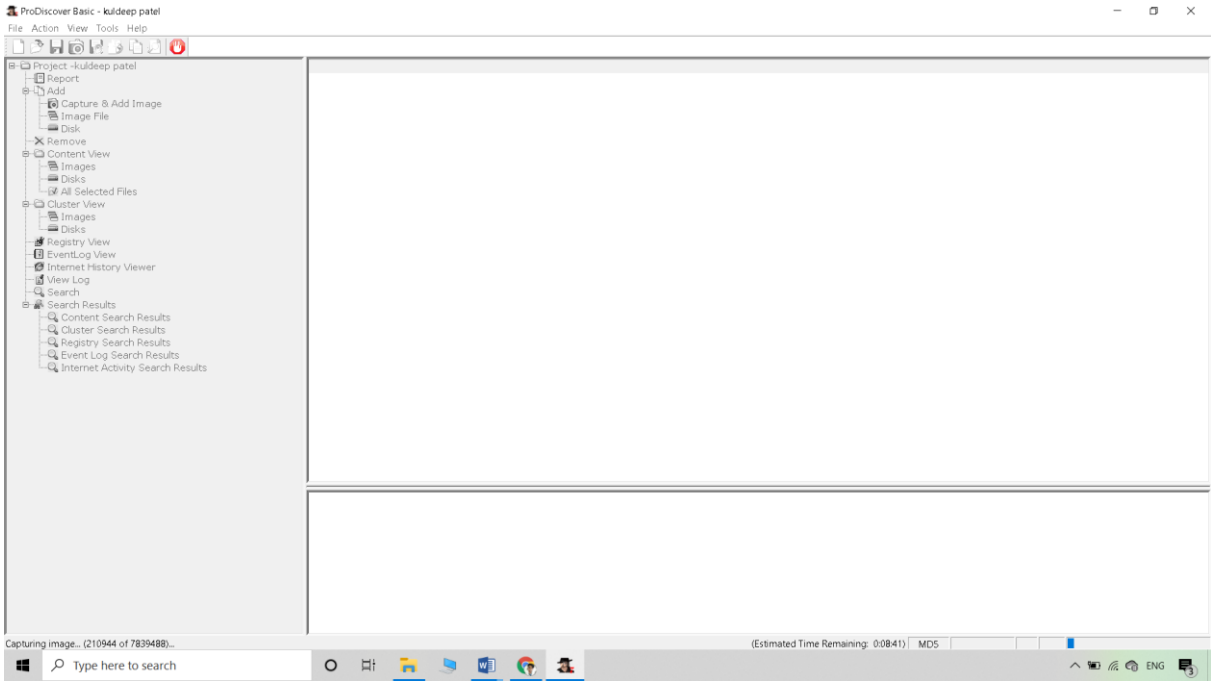
Practical 4

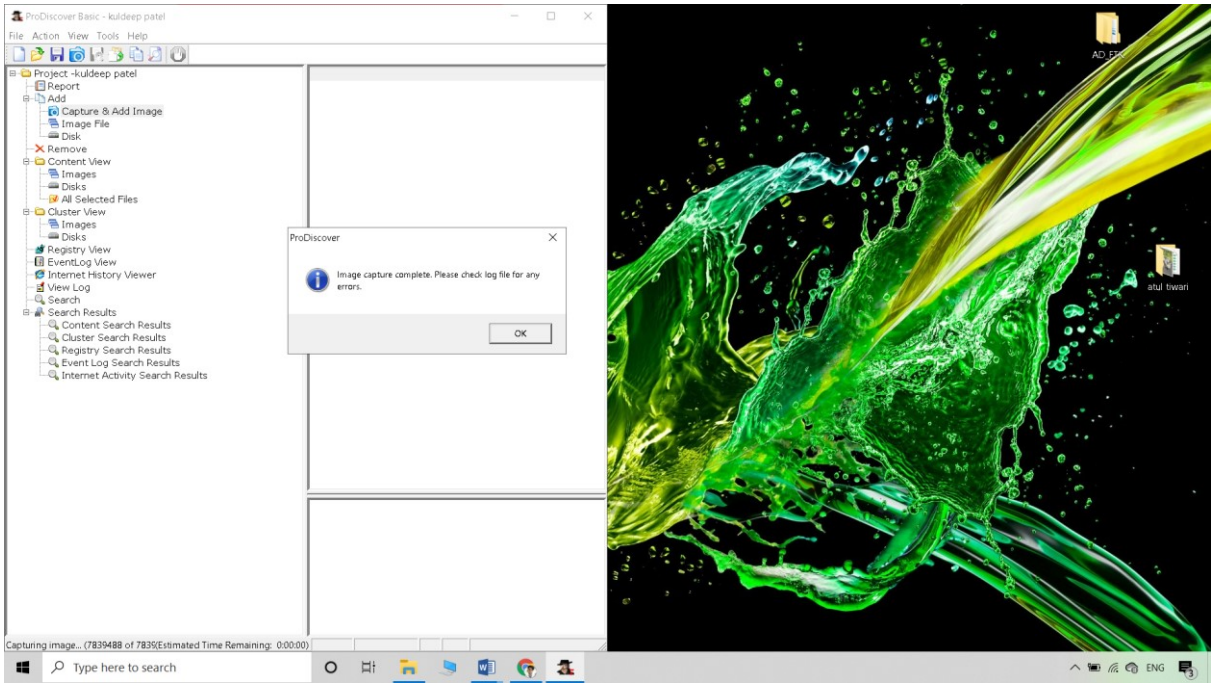
Aim: Data Acquisition:
- Perform data
acquisition using: - USB
Write Blocker + FTK
Imager
Steps:

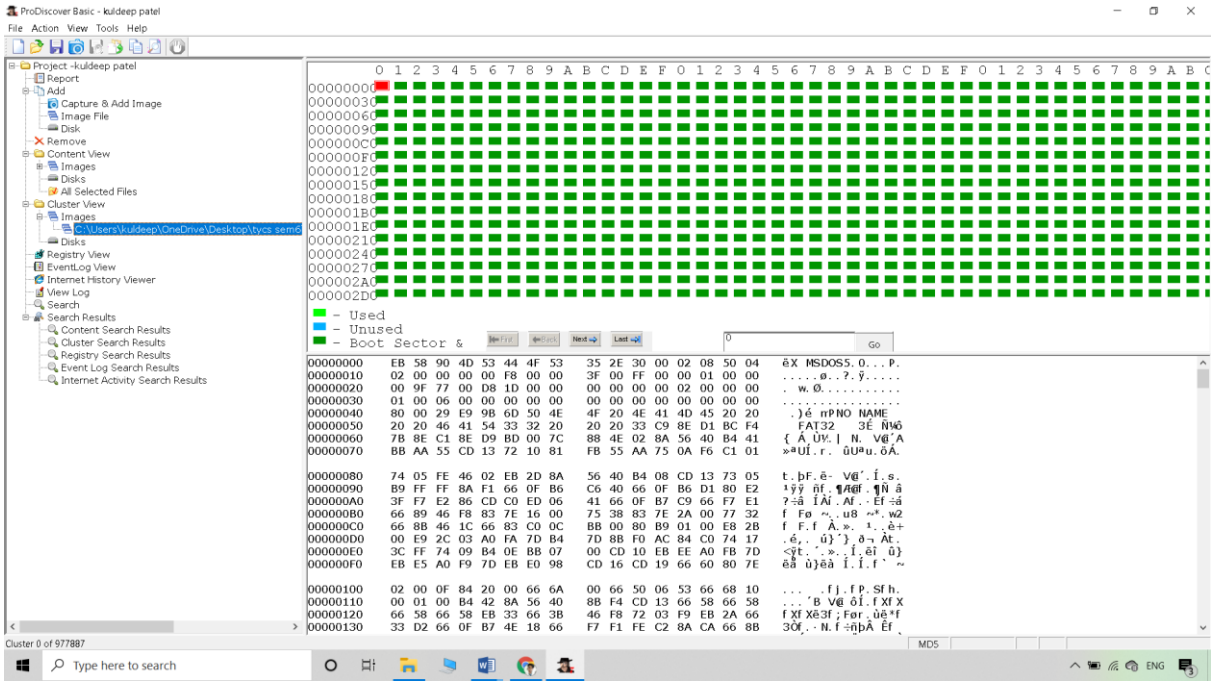
Step 1: First Open Prodiscover Basic and start with new case.

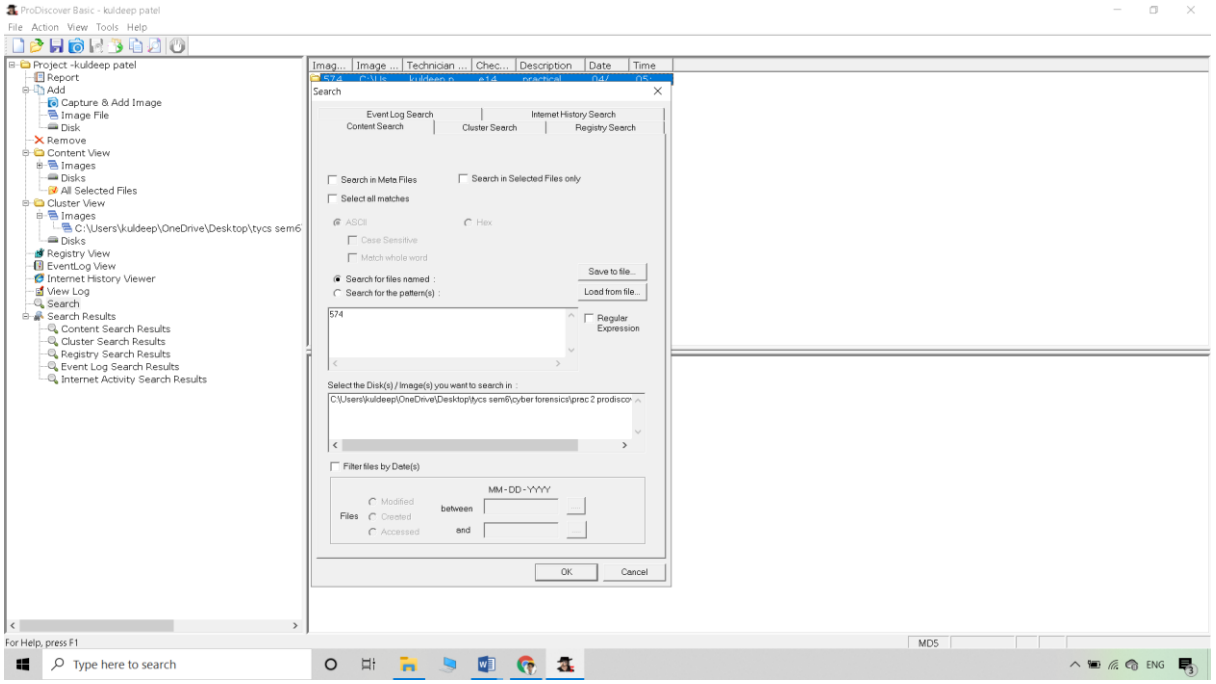



ProDiscover Basic - kuldeep patel
File Action View Tools Help
Project -kuldeep patel
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Internet Activity Search Results
Capture Image
Source Drive:
E:\ [KSP] 3.738 GB
Destination:
C:\Users\kuldeep\OneDrive\Des
>>
Split
Image Format:
ProDiscover Format (recommended)
Total sectors to capture :
7823104
HPA
Shadow Volume Name:
ProDiscover Image
Technician Name:
Image Number:
Description :
practical 2 kuldeep 574
Compression
Yes
No
Password...
OK
Cancel
AD_FR
atul tiwari
For Help, press F1
Type here to search
ENG


ProDiscover Basic - kuldeep patel
File Action View Tools Help
Project -kuldeep patel
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Internet Activity Search Results
Capturing image... (210944 of 7839488)...
(Estimated Time Remaining: 0:08:41)
MD5
Type here to search
ENG


ProDiscover Basic - kuldeep patel
File Action View Tools Help
Project -kuldeep patel
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Internet Activity Search Results
ProDiscover
Image capture complete. Please check log file for any errors.
OK
Capturing image... (7839488 of 7839(Estimated Time Remaining: 0:00:00)
Type here to search
ENG
AD_FPC
atul tiwari


ProDiscover Basic - kuldeep patel
File Action View Tools Help
Project -kuldeep patel
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
C:\Users\kuldeep\OneDrive\Desktop\tycs sem6
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Internet Activity Search Results
- Used
- Unused
- Boot Sector &
Go
Cluster 0 of 977887
MD5
Type here to search
ENG


ProDiscover Basic - kuldeep patel
File Action View Tools Help
Project -kuldeep patel
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
C:\Users\kuldeep\OneDrive\Desktop\tycs sem6
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Internet Activity Search Results
Imag... Image ... Technician ... Chec... Description Date Time
Search
Event Log Search
Internet History Search
Content Search
Cluster Search
Registry Search
Search in Meta Files
Search in Selected Files only
Select all matches
ASCII
Hex
Case Sensitive
Match whole word
Search for files named :
Search for the pattern(s) :
Save to file...
Load from file...
574
Regular Expression
Select the Disk(s) / Image(s) you want to search in :
C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics\prac 2 prodisco
Filter files by Date(s)
MM-DD-YYYY
Files
Modified
Created
Accessed
between
and
OK
Cancel
For Help, press F1
MD5
Type here to search
ENG

PRACTICAL 5

Aim :- Analyze the packets provided in lab and solve the questions using Wireshark :

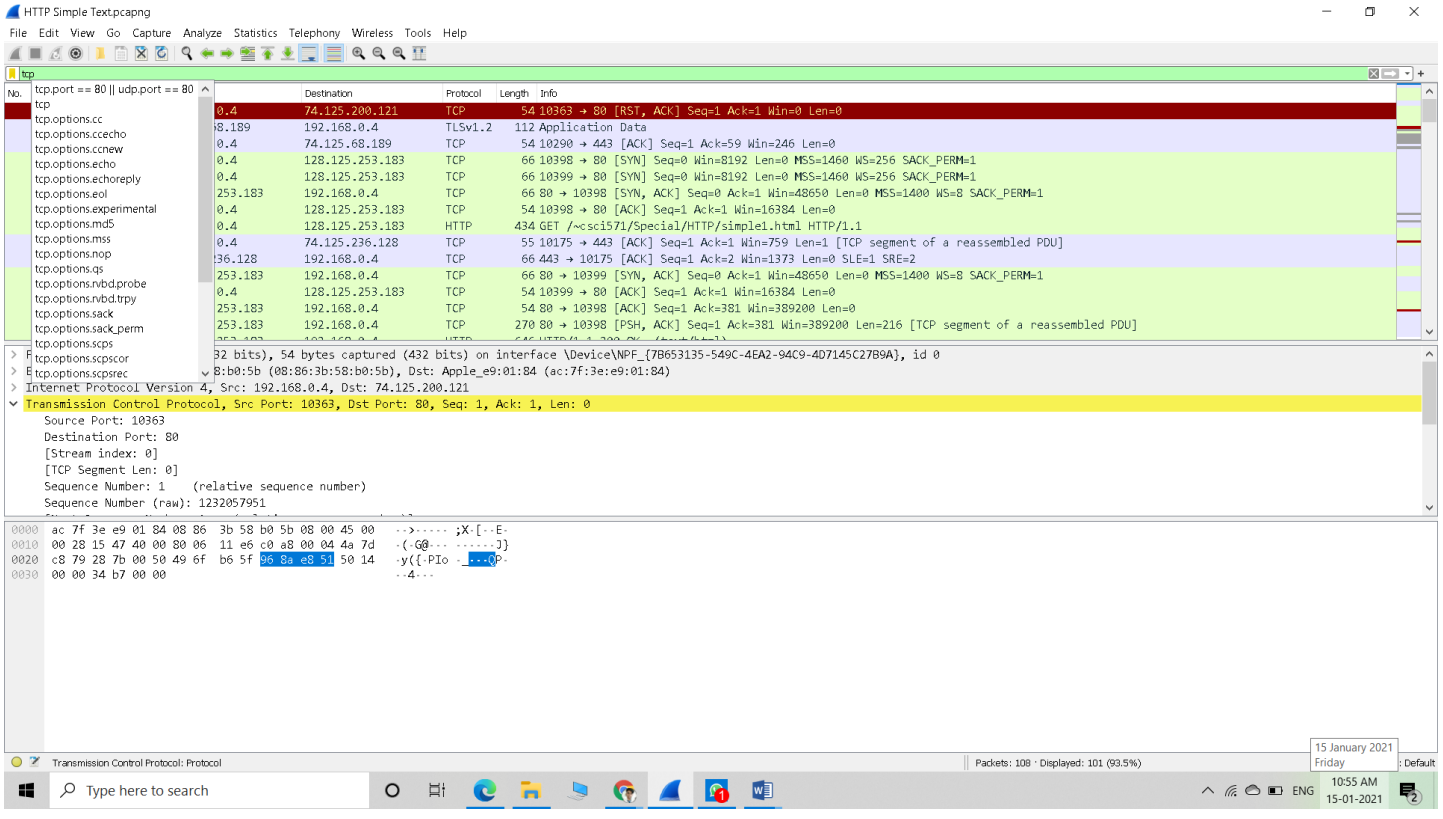
- What web server software is used by www.snopes.com?

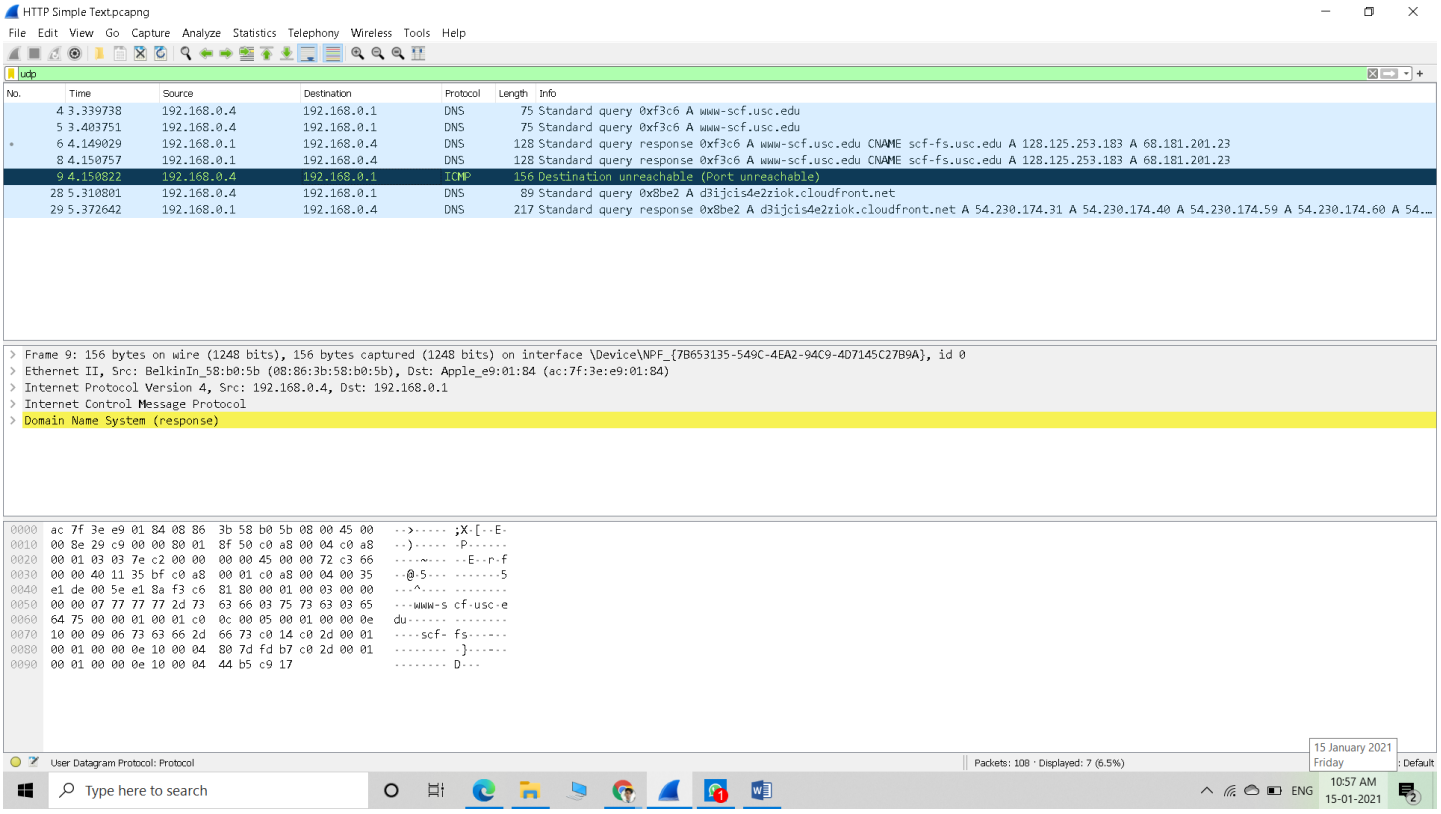
- About what cell phone problem is the client concerned? - According to Zillow, what instrument will Ryan learn to play?

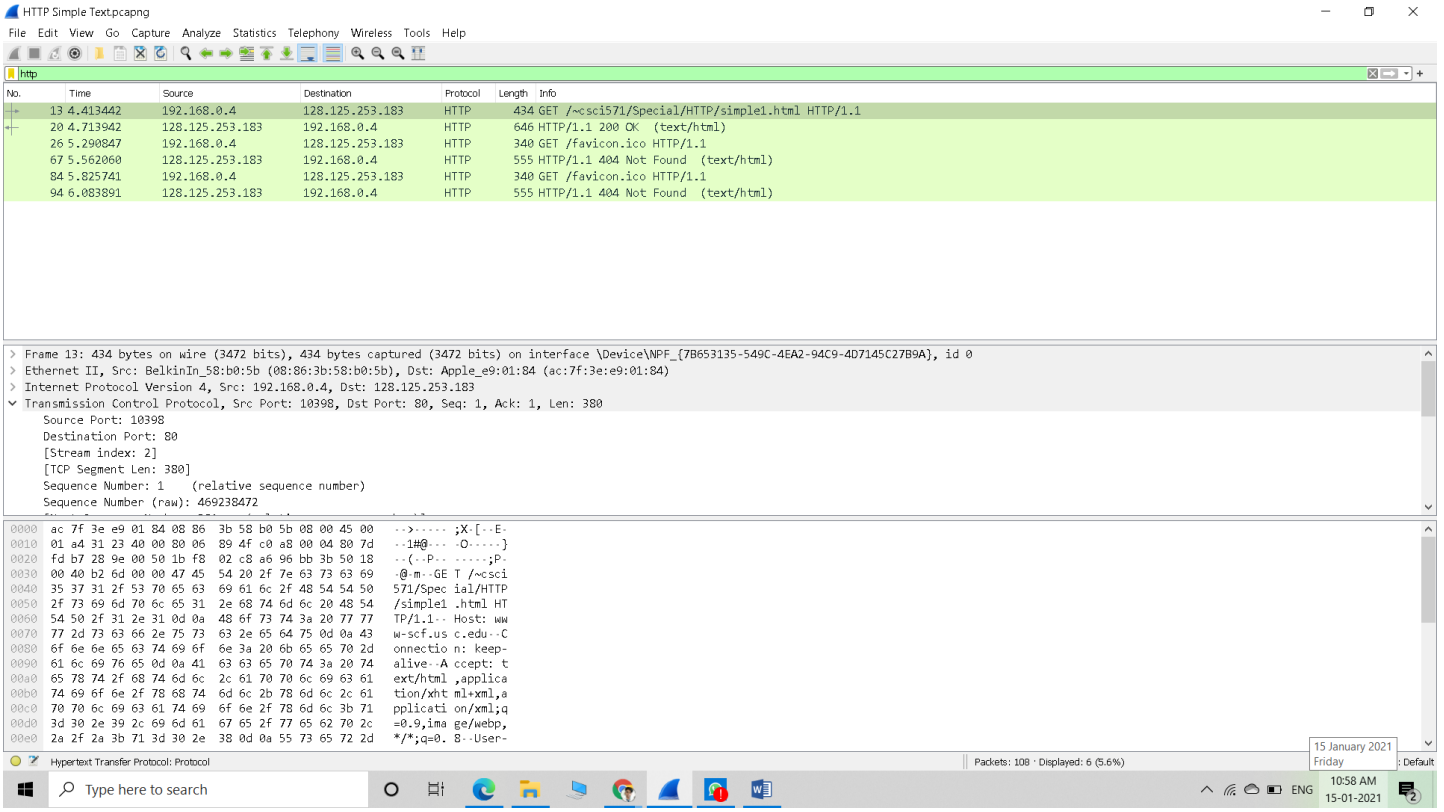
- How many web servers are running Apache?

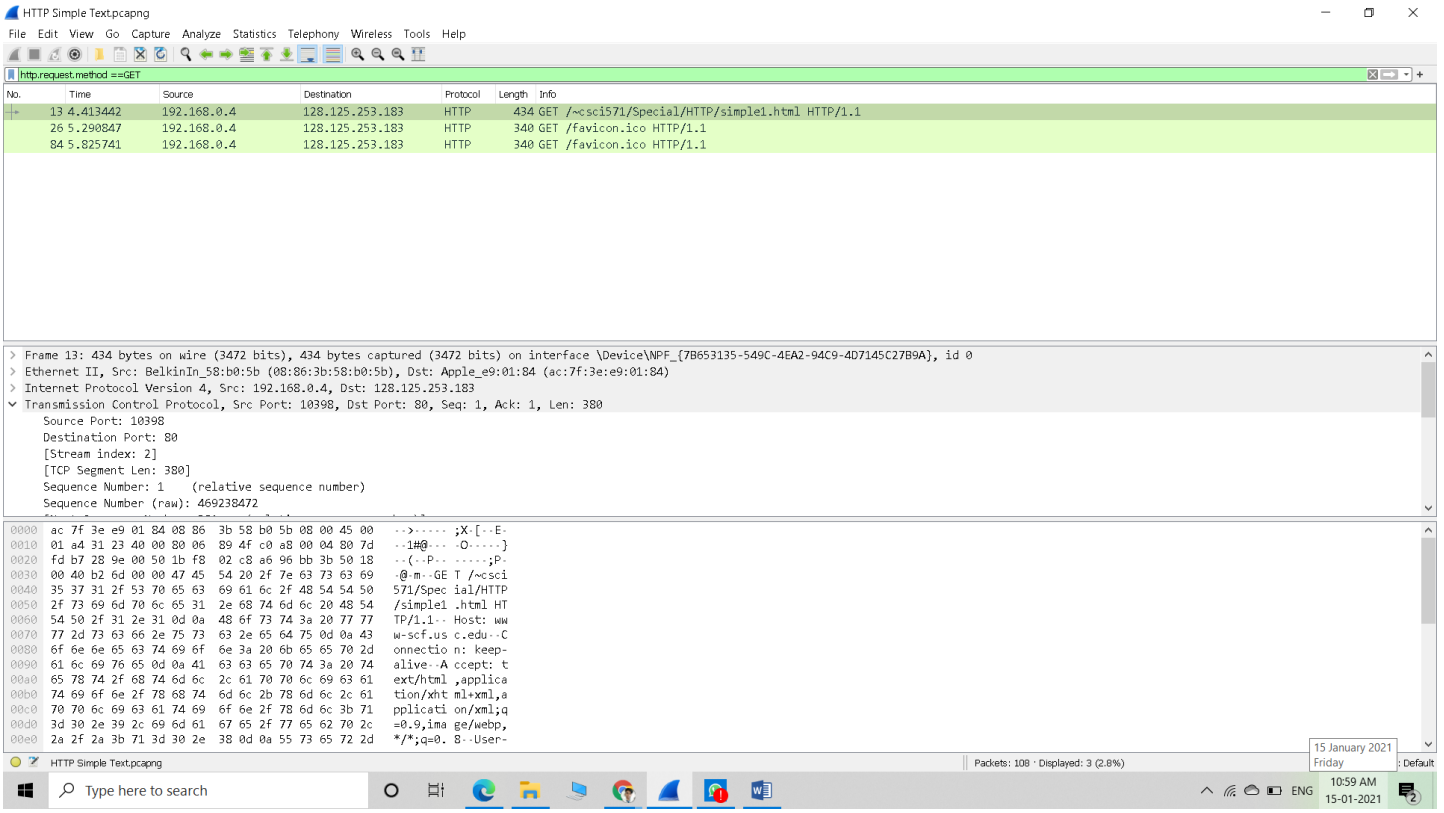
1. What web server software issued by www.snopes.com?

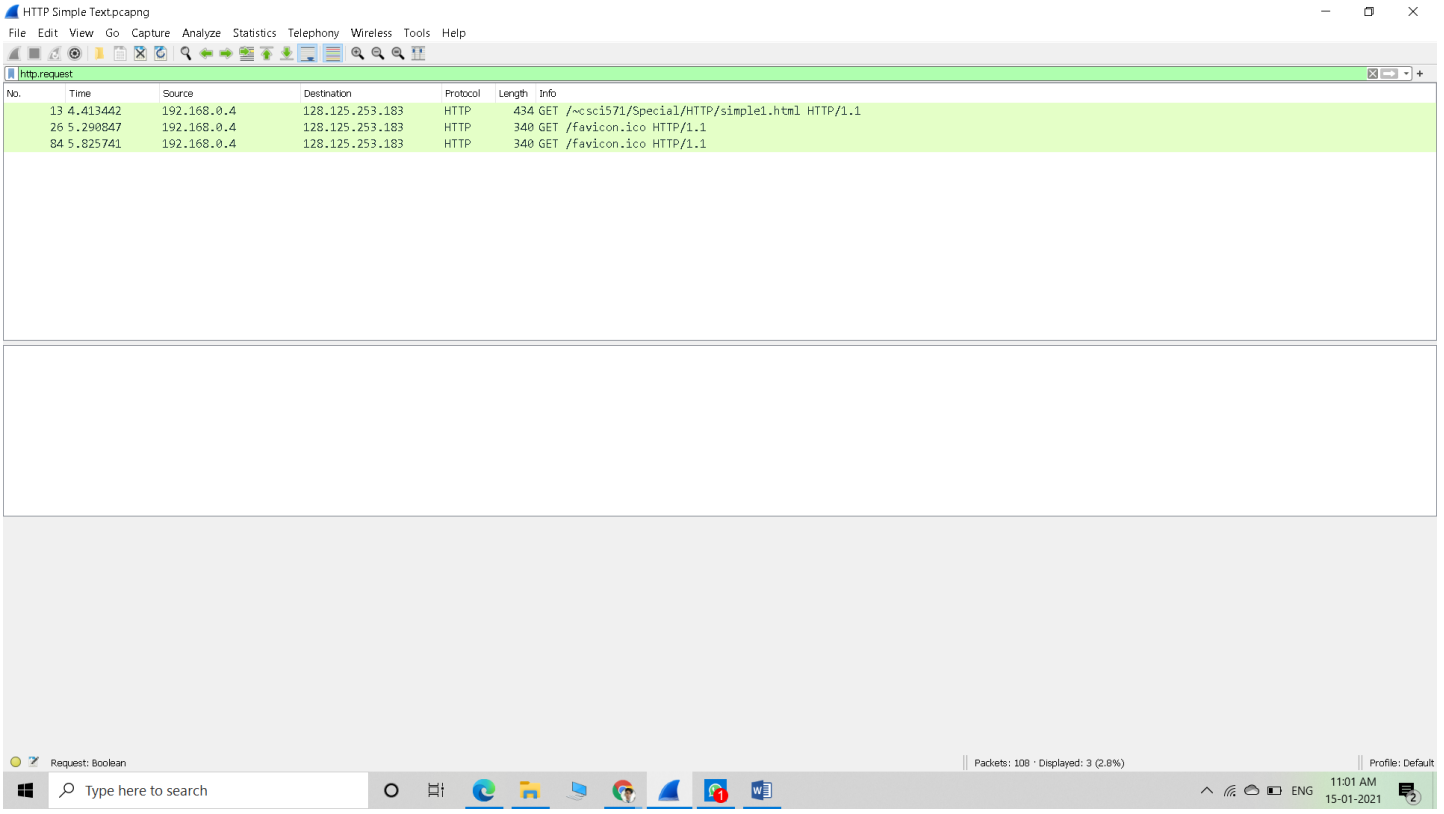
Analysis – The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column.

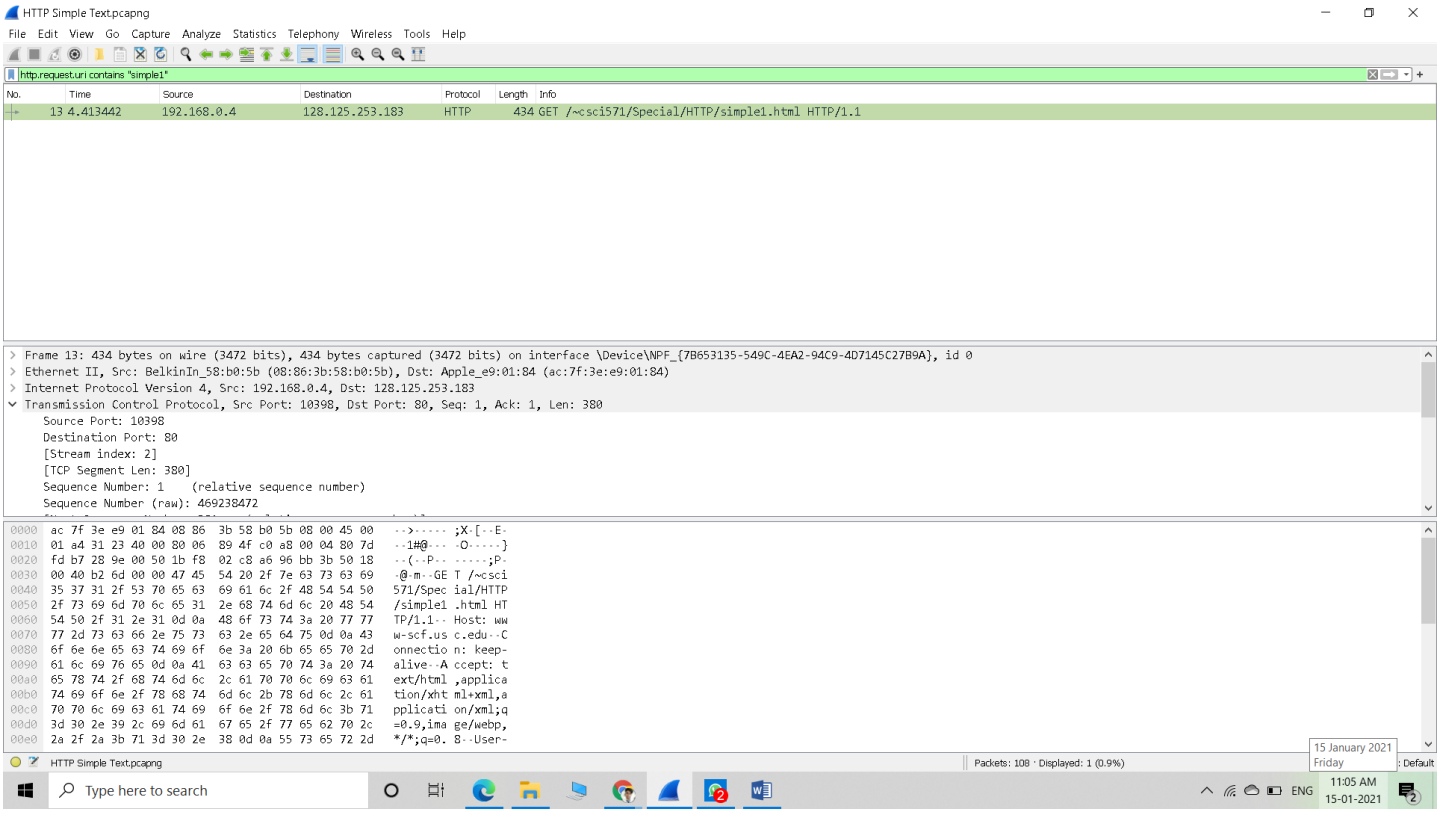


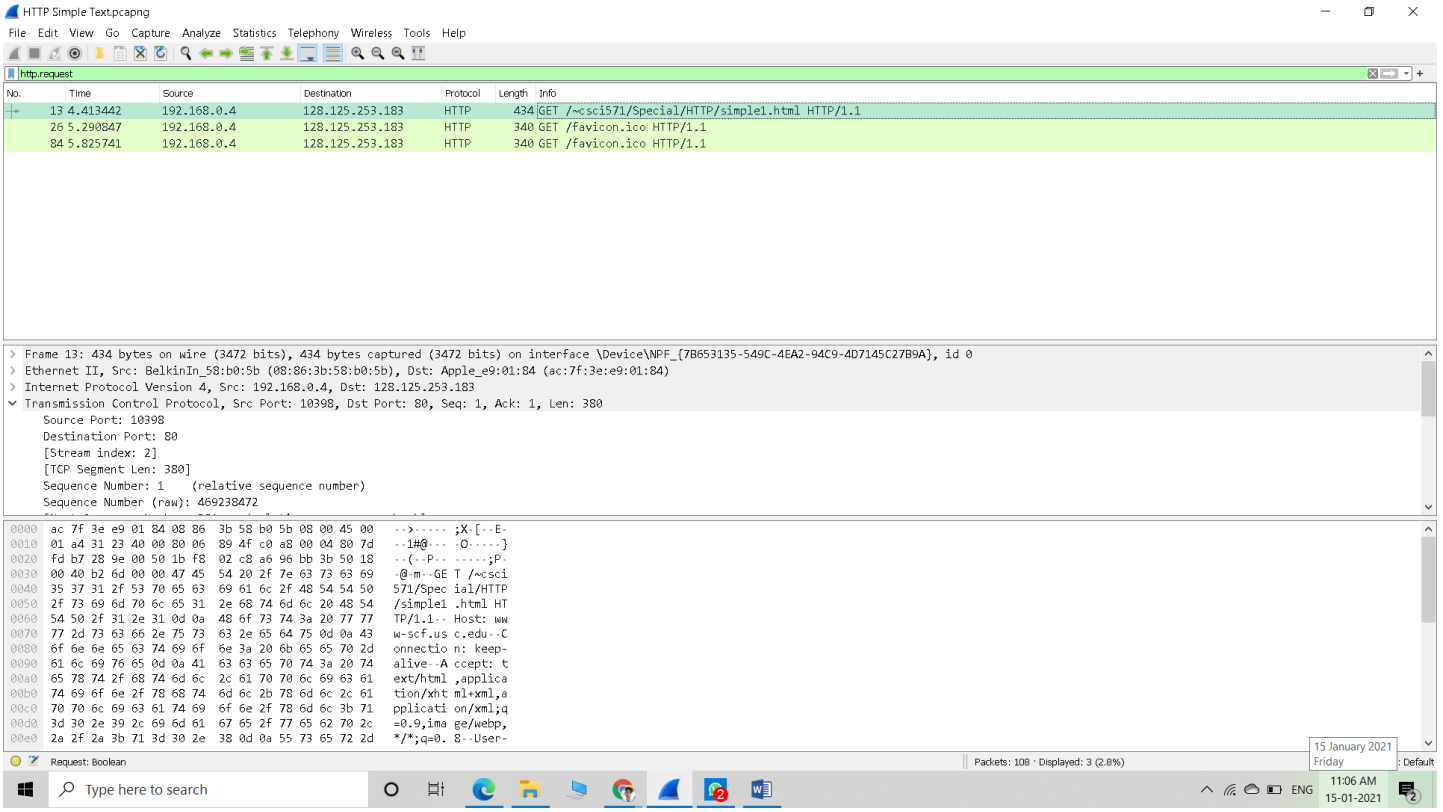

HTTP Simple Text.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
4 3.339738 192.168.0.4 192.168.0.1 DNS 75 Standard query 0xf3c6 A www-scf.usc.edu
5 3.403751 192.168.0.4 192.168.0.1 DNS 75 Standard query 0xf3c6 A www-scf.usc.edu
6 4.149029 192.168.0.1 192.168.0.4 DNS 128 Standard query response 0xf3c6 A www-scf.usc.edu CNAME scf-fs.usc.edu A 128.125.253.183 A 68.181.201.23
8 4.150757 192.168.0.1 192.168.0.4 DNS 128 Standard query response 0xf3c6 A www-scf.usc.edu CNAME scf-fs.usc.edu A 128.125.253.183 A 68.181.201.23
9 4.150822 192.168.0.4 192.168.0.1 ICMP 156 Destination unreachable (Port unreachable)
28 5.310801 192.168.0.4 192.168.0.1 DNS 89 Standard query 0x8be2 A d3ijcis4e2ziok.cloudfront.net
29 5.372642 192.168.0.1 192.168.0.4 DNS 217 Standard query response 0x8be2 A d3ijcis4e2ziok.cloudfront.net A 54.230.174.31 A 54.230.174.40 A 54.230.174.59 A 54.230.174.60 A 54.
Frame 9: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface \Device\NPF_{7B653135-549C-4EA2-94C9-4D7145C27B9A}, id 0
Ethernet II, Src: BelkinIn_58:b0:5b (08:86:3b:58:b0:5b), Dst: Apple_e9:01:84 (ac:7f:3e:e9:01:84)
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 192.168.0.1
Internet Control Message Protocol
Domain Name System (response)
0000 ac 7f 3e e9 01 84 08 86 3b 58 b0 5b 08 00 45 00
0010 00 8e 29 c9 00 00 80 01 8f 50 c0 a8 00 04 c0 a8
0020 00 01 03 03 7e c2 00 00 00 00 45 00 00 72 c3 66
0030 00 00 40 11 35 bf c0 a8 00 01 c0 a8 00 04 00 35
0040 e1 de 00 5e e1 8a f3 c6 81 80 00 01 00 03 00 00
0050 00 00 07 77 77 77 2d 73 63 66 03 75 73 63 03 65
0060 64 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 0e
0070 10 00 09 06 73 63 66 2d 66 73 c0 14 c0 2d 00 01
0080 00 01 00 00 0e 10 00 04 80 7d fd b7 c0 2d 00 01
0090 00 01 00 00 0e 10 00 04 44 b5 c9 17
User Datagram Protocol: Protocol
Packets: 108 · Displayed: 7 (6.5%)
15 January 2021
Friday
Type here to search
ENG
10:57 AM
15-01-2021


HTTP Simple Text.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
13 4.413442 192.168.0.4 128.125.253.183 HTTP 434 GET /~csci571/Special/HTTP/simple1.html HTTP/1.1
20 4.713942 128.125.253.183 192.168.0.4 HTTP 646 HTTP/1.1 200 OK (text/html)
26 5.290847 192.168.0.4 128.125.253.183 HTTP 340 GET /favicon.ico HTTP/1.1
67 5.562060 128.125.253.183 192.168.0.4 HTTP 555 HTTP/1.1 404 Not Found (text/html)
84 5.825741 192.168.0.4 128.125.253.183 HTTP 340 GET /favicon.ico HTTP/1.1
94 6.083891 128.125.253.183 192.168.0.4 HTTP 555 HTTP/1.1 404 Not Found (text/html)
Frame 13: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface \Device\NPF_{7B653135-549C-4EA2-94C9-4D7145C27B9A}, id 0
Ethernet II, Src: BelkinIn_58:b0:5b (08:86:3b:58:b0:5b), Dst: Apple_e9:01:84 (ac:7f:3e:e9:01:84)
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 128.125.253.183
Transmission Control Protocol, Src Port: 10398, Dst Port: 80, Seq: 1, Ack: 1, Len: 380
Source Port: 10398
Destination Port: 80
[Stream index: 2]
[TCP Segment Len: 380]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 469238472
0000 ac 7f 3e e9 01 84 08 86 3b 58 b0 5b 08 00 45 00
0010 01 a4 31 23 40 00 80 06 89 4f c0 a8 00 04 80 7d
0020 fd b7 28 9e 00 50 1b f8 02 c8 a6 96 bb 3b 50 18
0030 00 40 b2 6d 00 00 47 45 54 20 2f 7e 63 73 63 69
0040 35 37 31 2f 53 70 65 63 69 61 6c 2f 48 54 54 50
0050 2f 73 69 6d 70 6c 65 31 2e 68 74 6d 6c 20 48 54
0060 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77
0070 77 2d 73 63 66 2e 75 73 63 2e 65 64 75 0d 0a 43
0080 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d
0090 61 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 74
00a0 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61
00b0 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61
00c0 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71
00d0 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 70 2c
00e0 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 55 73 65 72 2d
Hypertext Transfer Protocol: Protocol
Packets: 108 · Displayed: 6 (5.6%)
Type here to search
ENG
10:58 AM
15-01-2021
15 January 2021
Friday


HTTP Simple Text.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method ==GET
No. Time Source Destination Protocol Length Info
13 4.413442 192.168.0.4 128.125.253.183 HTTP 434 GET /~csci571/Special/HTTP/simple1.html HTTP/1.1
26 5.290847 192.168.0.4 128.125.253.183 HTTP 340 GET /favicon.ico HTTP/1.1
84 5.825741 192.168.0.4 128.125.253.183 HTTP 340 GET /favicon.ico HTTP/1.1
Frame 13: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface \Device\NPF_{7B653135-549C-4EA2-94C9-4D7145C27B9A}, id 0
Ethernet II, Src: BelkinIn_58:b0:5b (08:86:3b:58:b0:5b), Dst: Apple_e9:01:84 (ac:7f:3e:e9:01:84)
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 128.125.253.183
Transmission Control Protocol, Src Port: 10398, Dst Port: 80, Seq: 1, Ack: 1, Len: 380
Source Port: 10398
Destination Port: 80
[Stream index: 2]
[TCP Segment Len: 380]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 469238472
0000 ac 7f 3e e9 01 84 08 86 3b 58 b0 5b 08 00 45 00
0010 01 a4 31 23 40 00 80 06 89 4f c0 a8 00 04 80 7d
0020 fd b7 28 9e 00 50 1b f8 02 c8 a6 96 bb 3b 50 18
0030 00 40 b2 6d 00 00 47 45 54 20 2f 7e 63 73 63 69
0040 35 37 31 2f 53 70 65 63 69 61 6c 2f 48 54 54 50
0050 2f 73 69 6d 70 6c 65 31 2e 68 74 6d 6c 20 48 54
0060 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77
0070 77 2d 73 63 66 2e 75 73 63 2e 65 64 75 0d 0a 43
0080 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d
0090 61 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 74
00a0 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61
00b0 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61
00c0 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71
00d0 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 70 2c
00e0 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 55 73 65 72 2d
HTTP Simple Text.pcapng
Packets: 108 · Displayed: 3 (2.8%)
Type here to search
ENG
10:59 AM
15-01-2021
15 January 2021
Friday

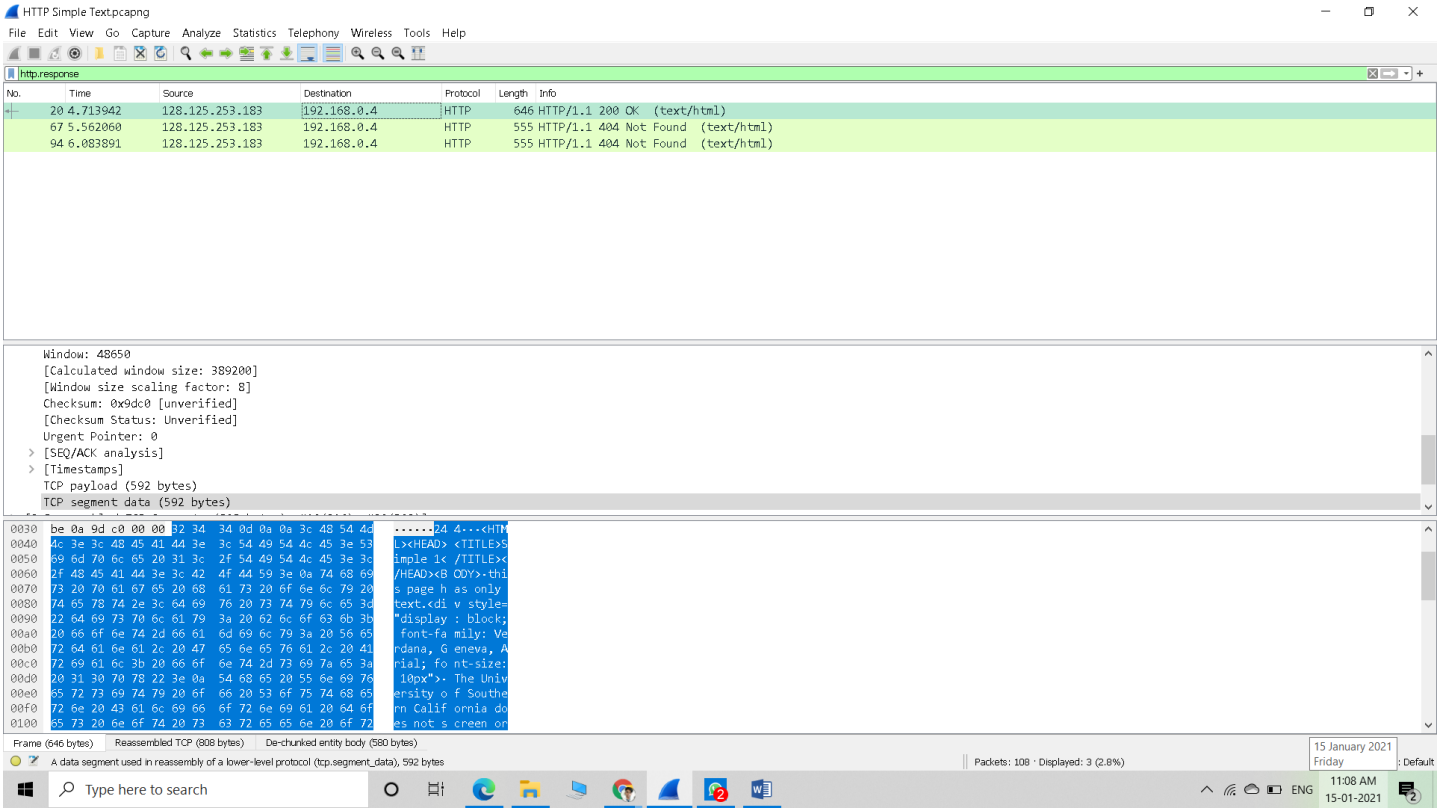

HTTP Simple Text.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
No. Time Source Destination Protocol Length Info
13 4.413442 192.168.0.4 128.125.253.183 HTTP 434 GET /~csci571/Special/HTTP/simple1.html HTTP/1.1
26 5.290847 192.168.0.4 128.125.253.183 HTTP 340 GET /favicon.ico HTTP/1.1
84 5.825741 192.168.0.4 128.125.253.183 HTTP 340 GET /favicon.ico HTTP/1.1
Request: Boolean
Packets: 108 · Displayed: 3 (2.8%)
Profile: Default
Type here to search
ENG
11:01 AM
15-01-2021


HTTP Simple Text.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.uri contains "simple1"
No. Time Source Destination Protocol Length Info
13 4.413442 192.168.0.4 128.125.253.183 HTTP 434 GET /~csci571/Special/HTTP/simple1.html HTTP/1.1
Frame 13: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface \Device\NPF_{7B653135-549C-4EA2-94C9-4D7145C27B9A}, id 0
Ethernet II, Src: BelkinIn_58:b0:5b (08:86:3b:58:b0:5b), Dst: Apple_e9:01:84 (ac:7f:3e:e9:01:84)
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 128.125.253.183
Transmission Control Protocol, Src Port: 10398, Dst Port: 80, Seq: 1, Ack: 1, Len: 380
Source Port: 10398
Destination Port: 80
[Stream index: 2]
[TCP Segment Len: 380]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 469238472
0000 ac 7f 3e e9 01 84 08 86 3b 58 b0 5b 08 00 45 00
0010 01 a4 31 23 40 00 80 06 89 4f c0 a8 00 04 80 7d
0020 fd b7 28 9e 00 50 1b f8 02 c8 a6 96 bb 3b 50 18
0030 00 40 b2 6d 00 00 47 45 54 20 2f 7e 63 73 63 69
0040 35 37 31 2f 53 70 65 63 69 61 6c 2f 48 54 54 50
0050 2f 73 69 6d 70 6c 65 31 2e 68 74 6d 6c 20 48 54
0060 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77
0070 77 2d 73 63 66 2e 75 73 63 2e 65 64 75 0d 0a 43
0080 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d
0090 61 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 74
00a0 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61
00b0 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61
00c0 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71
00d0 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 70 2c
00e0 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 55 73 65 72 2d
HTTP Simple Text.pcapng
Packets: 108 · Displayed: 1 (0.9%)
15 January 2021
Friday
Type here to search
ENG
11:05 AM
15-01-2021

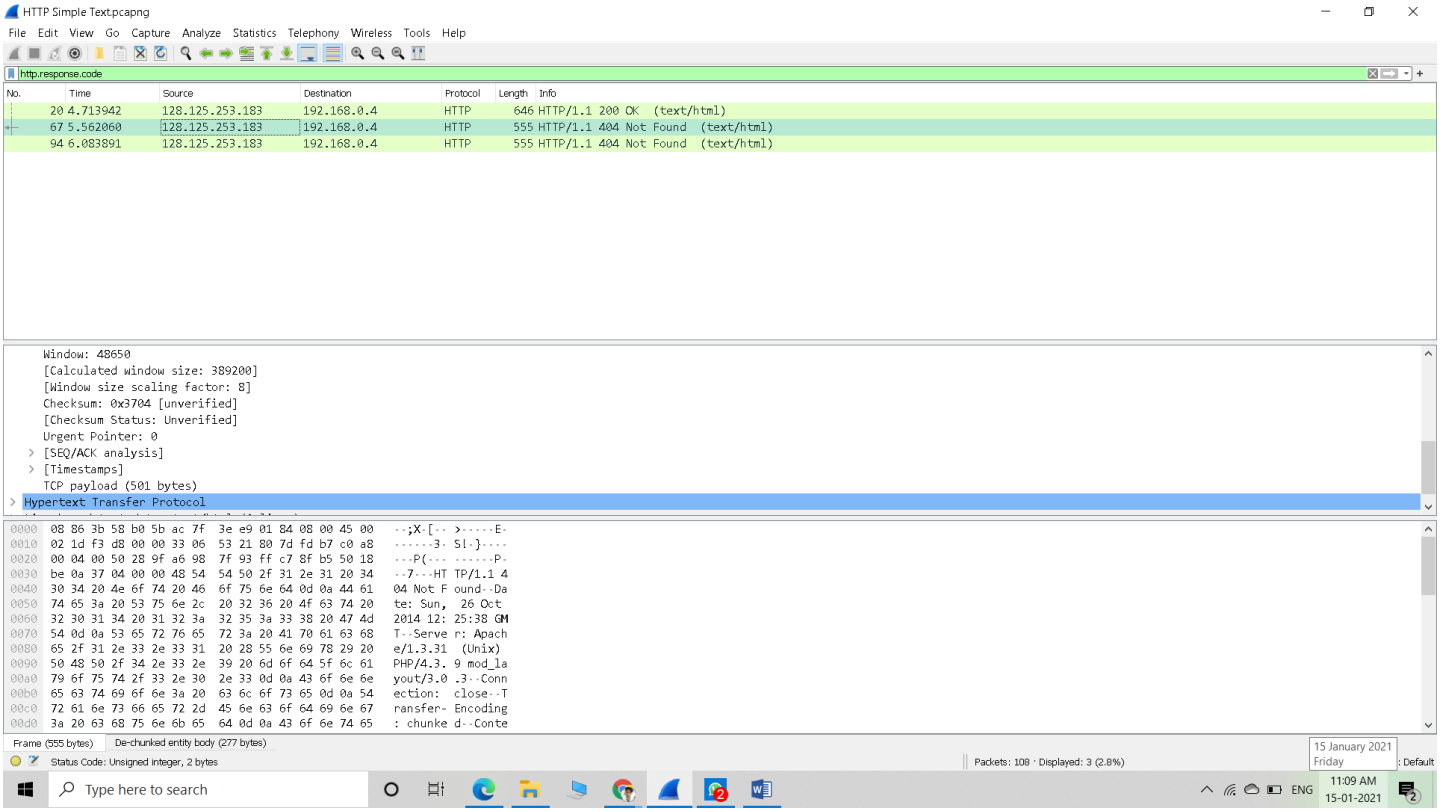


2. About what cell phone problem is the client concerned?

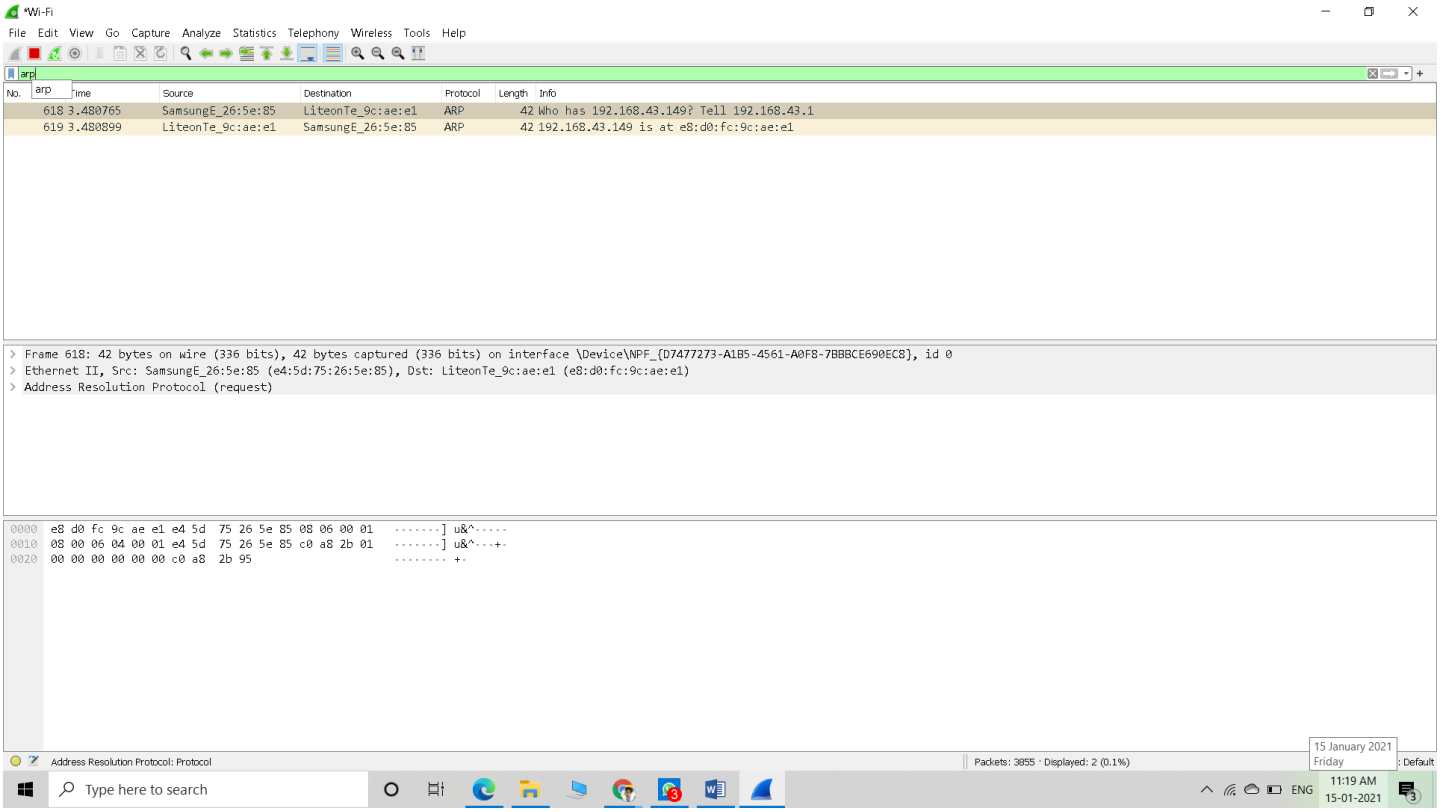
Analysis – Client talking about cell so we search for cell keyword in whole packets. We will use regular express for searching the cell keyword. Apply frame matches “(?i) cell”

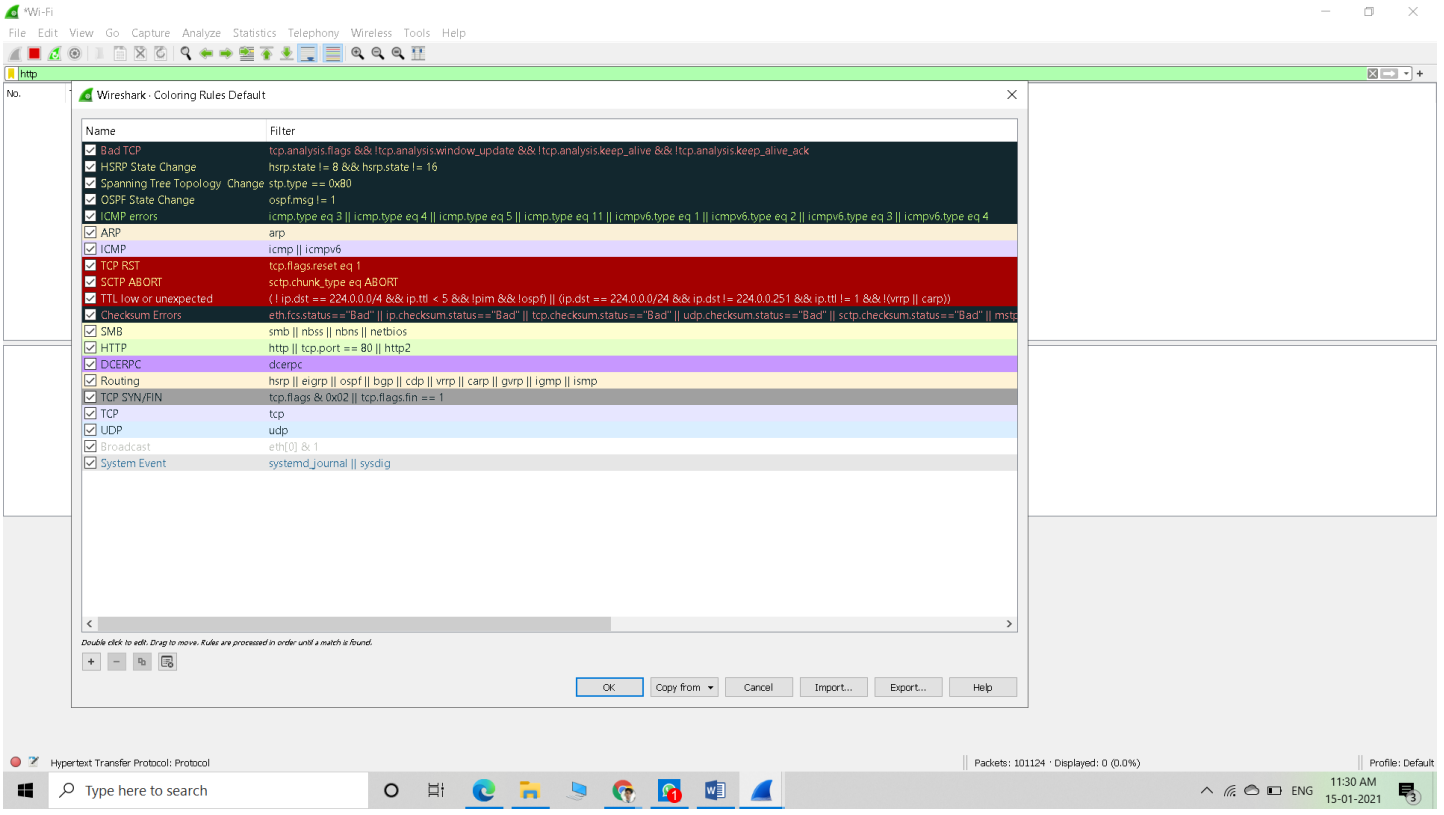


After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request cell keyword is in URL and it was about cell phone charging issue



3. According to Zillow, what instrument will Ryan learn to play? Analysis – As we did in the last challenge, we will apply a regular express filter for the 4. How many web servers are running Apache? Analysis – The web server name can be retrieved from HTTP response header. So will apply filter http. response and we can see all http response packets.illow keyword. Apply frame matched “(?!) zillow”


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
618 3.480765 SamsungE_26:5e:85 LiteonTe_9c:ae:e1 ARP 42 Who has 192.168.43.149? Tell 192.168.43.1
619 3.480899 LiteonTe_9c:ae:e1 SamsungE_26:5e:85 ARP 42 192.168.43.149 is at e8:d0:fc:9c:ae:e1
Frame 618: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D7477273-A1B5-4561-A0F8-7BBBCE690EC8}, id 0
Ethernet II, Src: SamsungE_26:5e:85 (e4:5d:75:26:5e:85), Dst: LiteonTe_9c:ae:e1 (e8:d0:fc:9c:ae:e1)
Address Resolution Protocol (request)
0000 e8 d0 fc 9c ae e1 e4 5d 75 26 5e 85 08 06 00 01
0010 08 00 06 04 00 01 e4 5d 75 26 5e 85 c0 a8 2b 01
0020 00 00 00 00 00 00 c0 a8 2b 95
Address Resolution Protocol: Protocol
Packets: 3855 · Displayed: 2 (0.1%)
Profile: Default
15 January 2021
Friday
Type here to search
ENG
11:19 AM
15-01-2021


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No.
Wireshark · Coloring Rules Default
Name Filter
Bad TCP tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
HSRP State Change hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change stp.type == 0x80
OSPF State Change ospf.msg != 1
ICMP errors icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4
ARP arp
ICMP icmp || icmpv6
TCP RST tcp.flags.reset eq 1
SCTP ABORT sctp.chunk_type eq ABORT
TTL low or unexpected (! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))
Checksum Errors eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || mstp
SMB smb || nbss || nbns || netbios
HTTP http || tcp.port == 80 || http2
DCERPC dcerpc
Routing hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN tcp.flags & 0x02 || tcp.flags.fin == 1
TCP tcp
UDP udp
Broadcast eth[0] & 1
System Event systemd_journal || sysdig
Double click to edit. Drag to move. Rules are processed in order until a match is found.
OK
Copy from
Cancel
Import...
Export...
Help
Hypertext Transfer Protocol: Protocol
Packets: 101124 · Displayed: 0 (0.0%)
Profile: Default
Type here to search
ENG
11:30 AM
15-01-2021

Practical 6

Aim :- Using Sysinternals tools for Network Tracking and Process Monitoring :

- Check Sysinternals tools
- Monitor Live Processes
- Capture RAM
- Capture TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

¬ Check Sysinternals tools : Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment.

The following are the categories of Sysinternals Tools:

1. File and Disk Utilities
2. Networking Utilities
3. Process Utilities
4. Security Utilities
5. System Information Utilities
6. Miscellaneous Utilities

¬ Monitor Live Processes : (Tool: ProcMon)

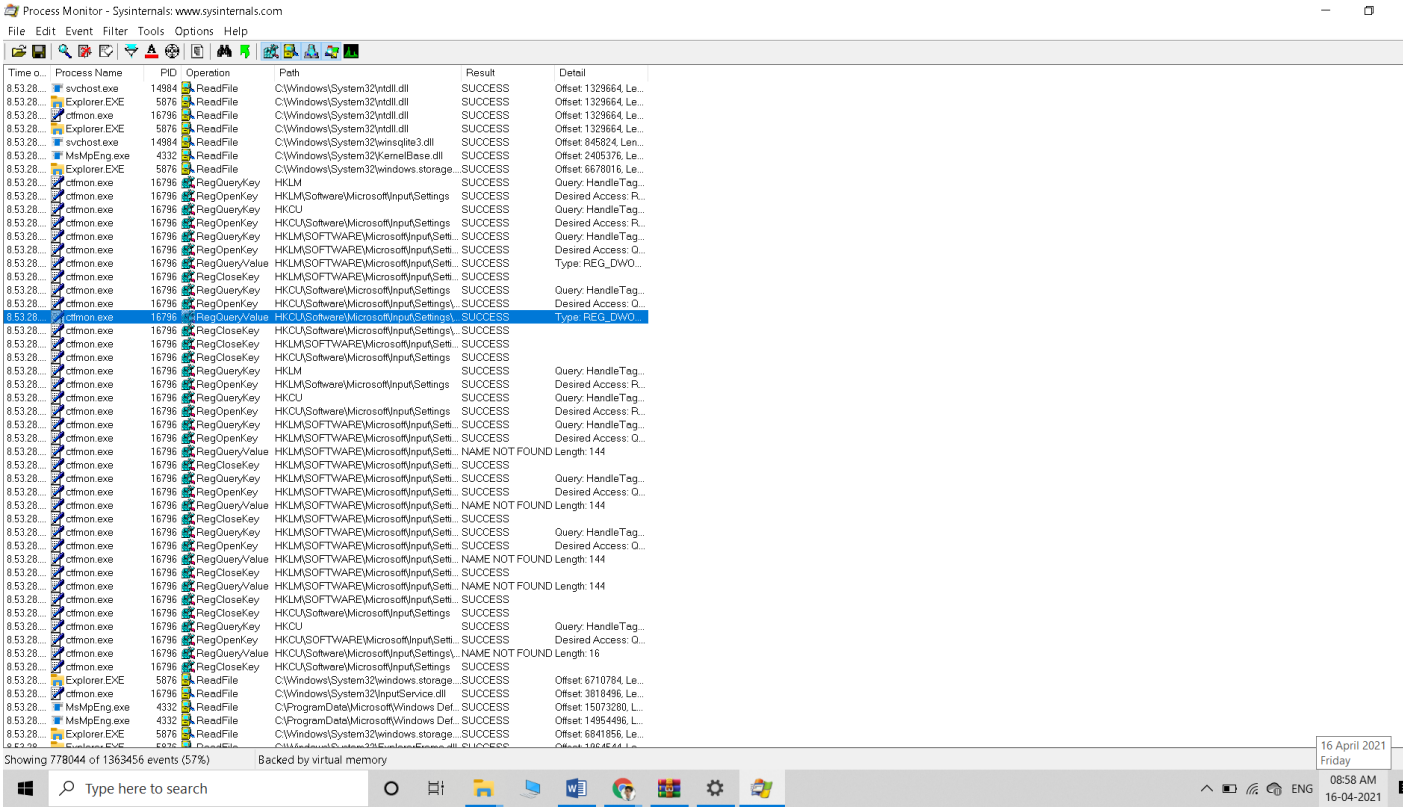
To Do:

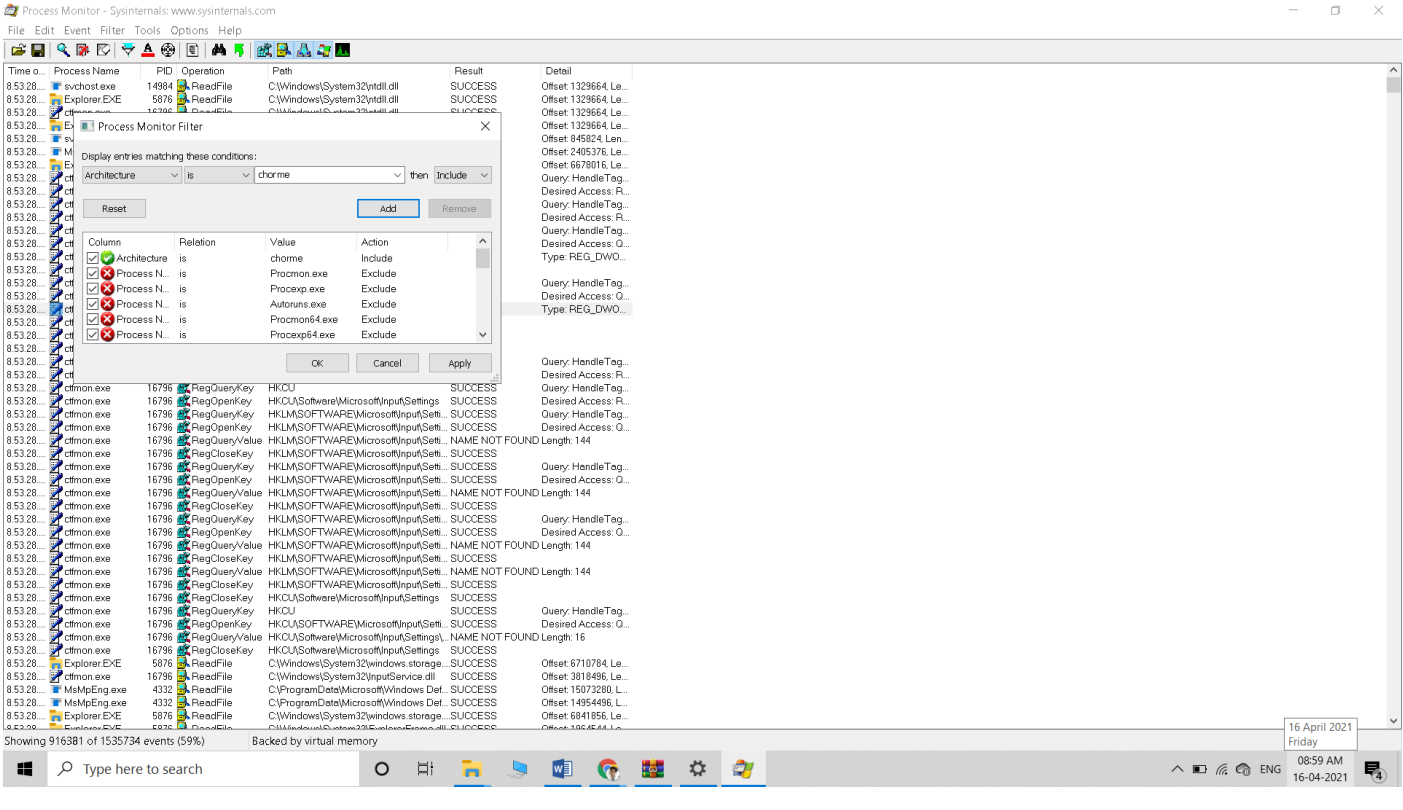
1. Filter (Process Name or PID or Architecture, etc)
2. Process Tree
3. Process Activity Summary
4. Count Occurrences

1) Monitor Live Processes : (Tool : ProcMon)

>Process Monitor, or ProcMon, is a Windows tool designed to help log application issues on your computer.

> With Process Monitor you can observe, view, and capture Windows file and system activity in real-time.

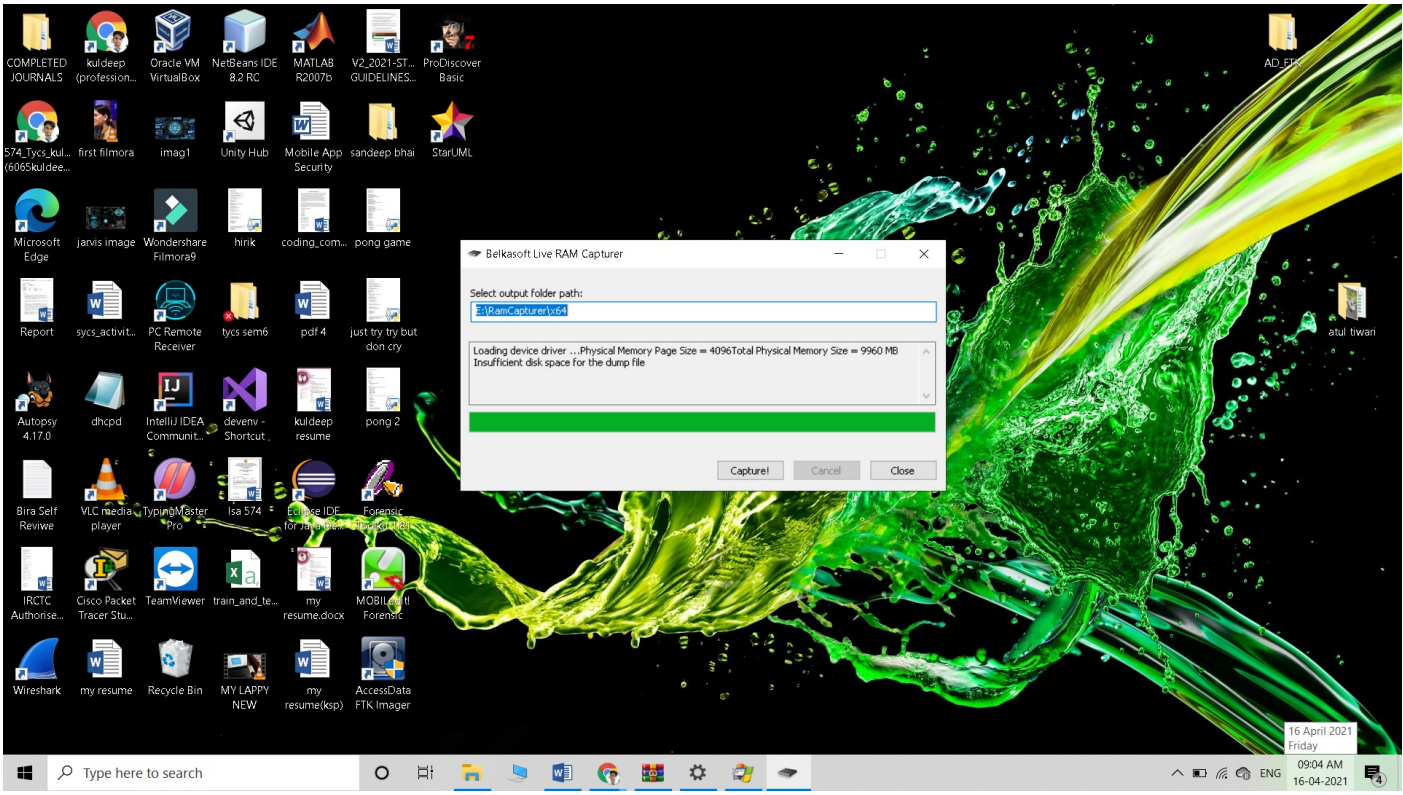

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
Showing 778044 of 1363456 events (57%)
Backed by virtual memory
Type here to search
16 April 2021
Friday
08:58 AM
16-04-2021


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Process Monitor Filter
Display entries matching these conditions:
Architecture is chorme then Include
Reset Add Remove
Column Relation Value Action
Architecture is chorme Include
Process N... is Procmon.exe Exclude
Process N... is Procexp.exe Exclude
Process N... is Autoruns.exe Exclude
Process N... is Procmon64.exe Exclude
Process N... is Procexp64.exe Exclude
OK Cancel Apply
Showing 916381 of 1535734 events (59%)
Backed by virtual memory
Type here to search
16 April 2021
Friday
08:59 AM
16-04-2021

2) Capture RAM (Tool : RAMCapture)

Magnet RAM Capture is a free imaging tool designed to capture the physical memory of a suspect's computer.

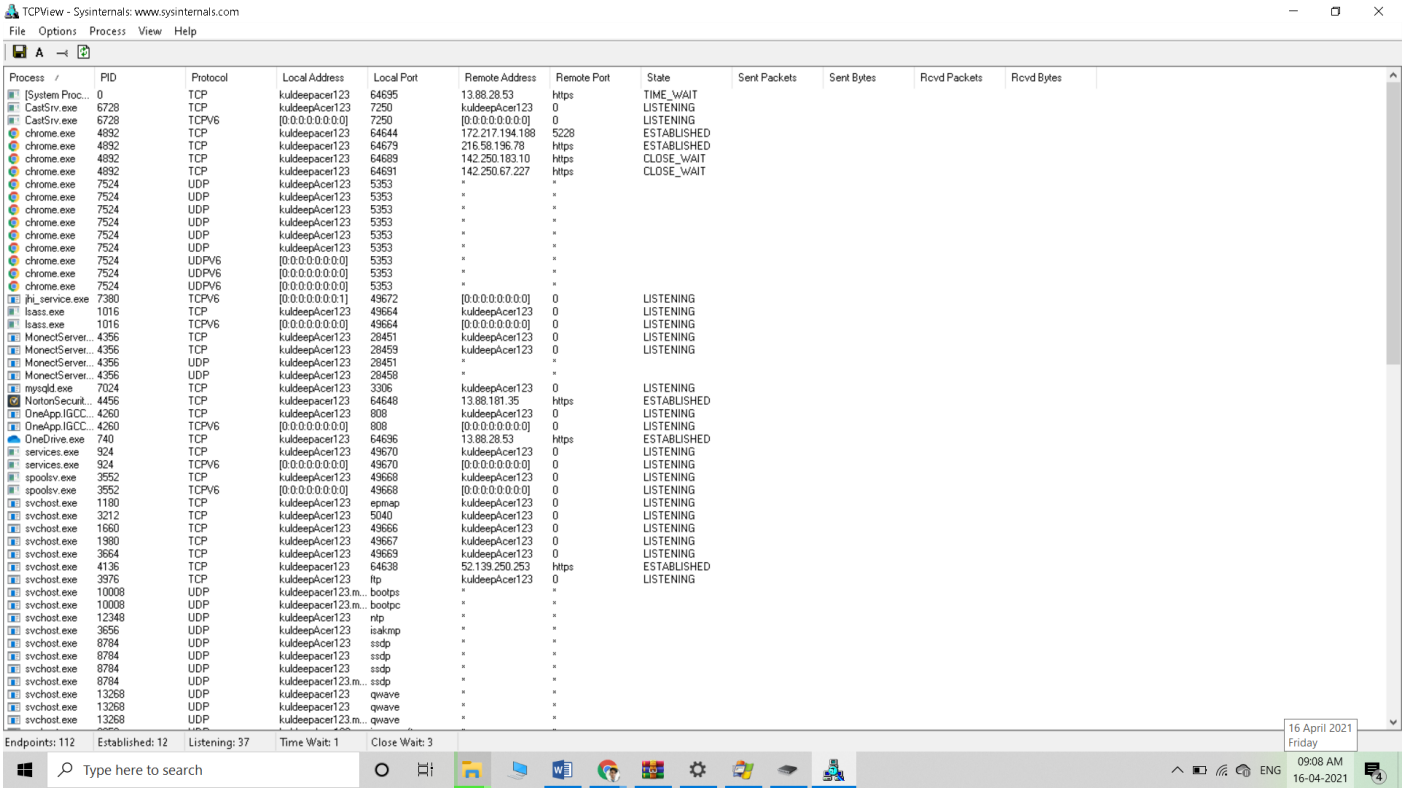
>allowing investigators to recover and analyze valuable artifacts that are often only found in memory.



3) Capture TCP/UDP packets (Tool : TcpView)

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system.

>including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint.



4) Monitor Hard Disk (Tool : DiskMon)

DiskMon is an application that logs and displays all hard disk activity on a Windows system.

>You can also minimize DiskMon to your system tray where it acts as a disk light, presenting a green icon

>when there is disk-read activity and a red icon when there is disk-write activity.

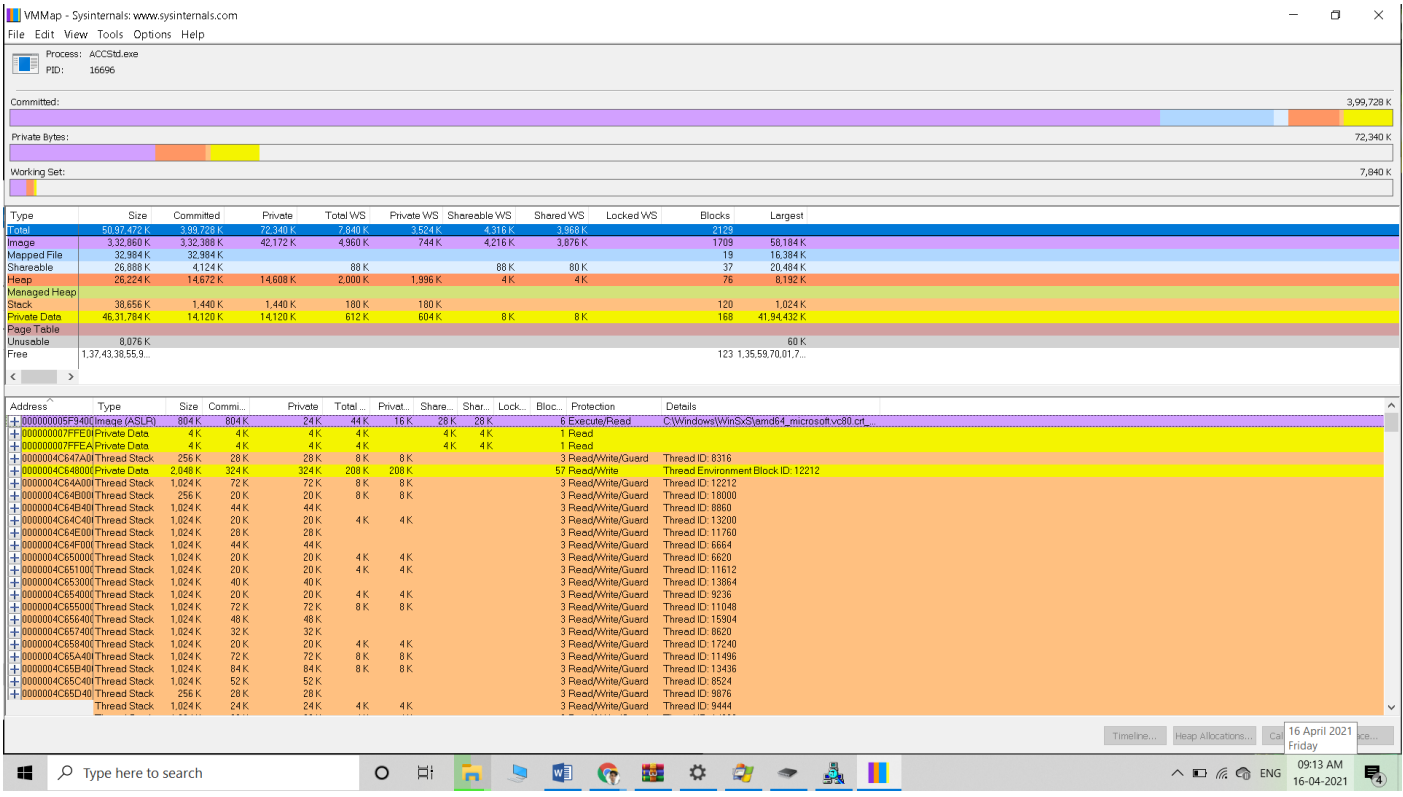
#	Time	Duration (s)	Disk	Request	Sector	Length
1099	41.520053	0.00000000	0	Write	247707136	64
1100	41.520121	0.00000000	0	Write	247538400	32
1101	41.520187	0.00000000	0	Write	17883760	44
1102	41.520989	0.00000000	0	Write	443480	8
1103	41.942999	0.00000000	0	Write	51931520	64
1104	42.625428	0.00000000	0	Write	51931584	64
1105	42.899951	0.00000000	0	Write	385816	8
1106	42.949897	0.00000000	0	Write	51931648	64
1107	43.628496	0.00000000	0	Write	51931712	64
1108	43.809943	0.00000000	0	Write	6496112	200
1109	43.810209	0.00000000	0	Write	6369488	8
1110	43.810244	0.00000000	0	Write	6369488	8
1111	43.810321	0.00000000	0	Write	6369472	8
1112	44.011271	0.00000000	0	Write	51931776	64
1113	44.260728	0.00000000	0	Write	45524856	4
1114	44.261386	0.00000000	0	Write	379832	8
1115	44.578563	0.00000000	0	Write	222791872	160
1116	44.597628	0.00000000	0	Read	284971992	128
1117	45.047863	0.00000000	0	Write	51931840	64
1118	45.203691	0.00000000	0	Read	79040352	64
1119	45.203892	0.00000000	0	Write	247707200	64
1120	45.203965	0.00000000	0	Write	247538400	32
1121	45.204117	0.00000000	0	Write	79040336	64
1122	45.204345	0.00000000	0	Write	6369616	16
1123	45.204379	0.00000000	0	Write	6369616	16
1124	45.623809	0.00000000	0	Write	343224	8
1125	45.624634	0.00000000	0	Read	2742560	32
1126	45.624739	0.00000000	0	Write	247707264	32
1127	45.624872	0.00000000	0	Write	247538400	32
1128	45.625032	0.00000000	0	Write	2742048	532
1129	46.089651	0.00000000	0	Write	51931904	64
1130	46.669656	0.00000000	0	Write	51931968	64
1131	46.975632	0.00000000	0	Write	6369496	8
1132	46.975911	0.00000000	0	Read	18142464	32
1133	46.976026	0.00000000	0	Write	247707296	32
1134	46.976128	0.00000000	0	Write	247538400	32
1135	46.976273	0.00000000	0	Write	18142480	46
1136	46.976832	0.00000000	0	Write	329080	8
1137	47.114971	0.00000000	0	Write	51932032	64
1138	48.145395	0.00000000	0	Write	51932096	64
1139	48.348314	0.00000000	0	Write	327040	8
1140	48.829667	0.00000000	0	Write	95476712	8
1141	49.129200	0.00000000	0	Write	51932160	64
1142	49.163428	0.00000000	0	Write	51932224	64
1143	49.711072	0.00000000	0	Write	19954480	16

5) Monitor Vitual Memory (Tool : VMMAP)

>VMMap is a process virtual and physical memory analysis utility.

>It shows a breakdown of a process's committed virtual memory

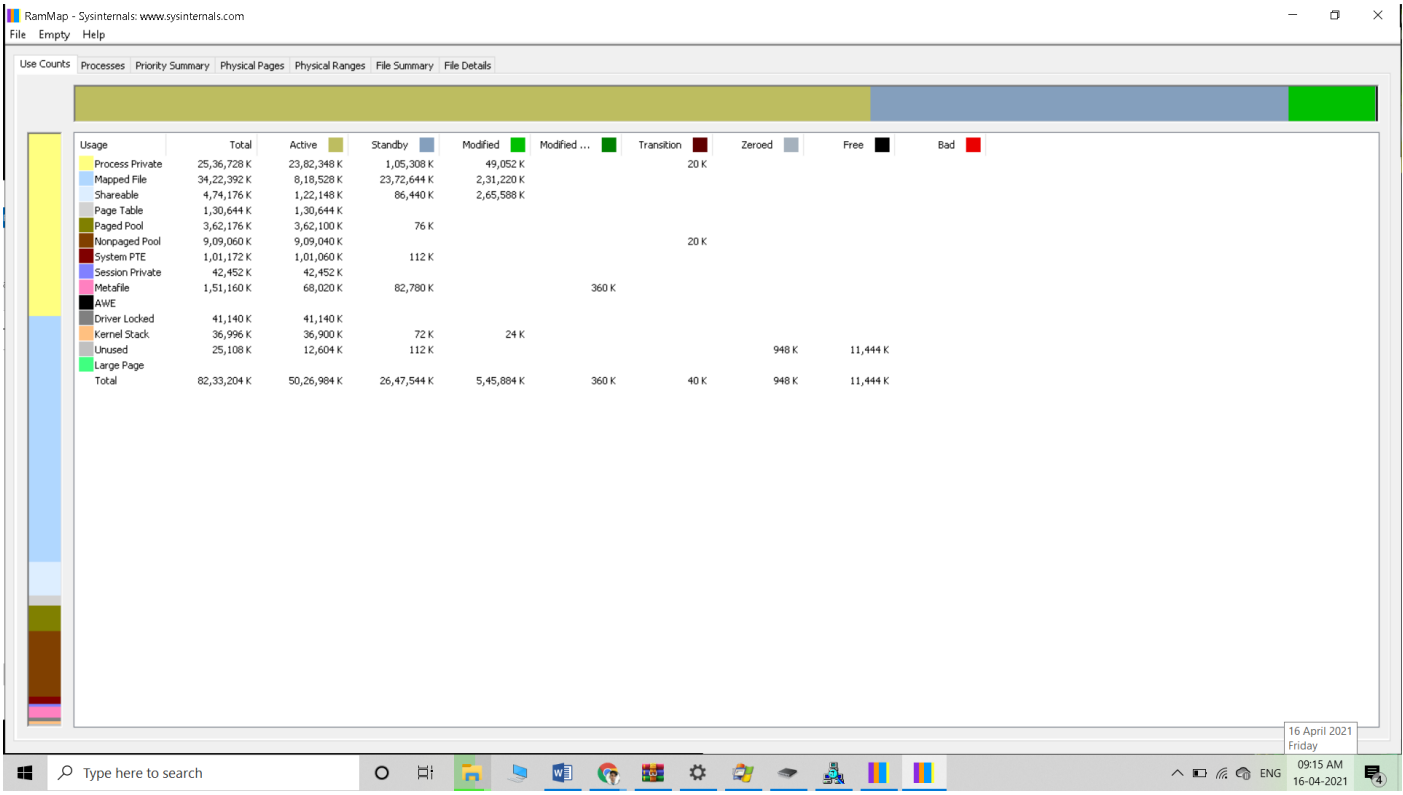
>types as well as the amount of physical memory (working set) assigned by the operating system to those types.



6) Monitor Cache Memory (Tool : RAMMap)

>RAMMap is a portable, stand-alone software tool that allows you to see exactly how Windows assigns physical memory.

>The tool does not just display memory usage on an application or process basis, but it shows the the memory usage down to each individual file.


RamMap - Sysinternals: www.sysinternals.com
File Empty Help
Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details
Usage Total Active Standby Modified Modified ... Transition Zeroed Free Bad
Process Private 25,36,728 K 23,82,348 K 1,05,308 K 49,052 K 20 K
Mapped File 34,22,392 K 8,18,528 K 23,72,644 K 2,31,220 K
Shareable 4,74,176 K 1,22,148 K 86,440 K 2,65,588 K
Page Table 1,30,644 K 1,30,644 K
Paged Pool 3,62,176 K 3,62,100 K 76 K
Nonpaged Pool 9,09,060 K 9,09,040 K 20 K
System PTE 1,01,172 K 1,01,060 K 112 K
Session Private 42,452 K 42,452 K
Metafile 1,51,160 K 68,020 K 82,780 K 360 K
AWE
Driver Locked 41,140 K 41,140 K
Kernel Stack 36,996 K 36,900 K 72 K 24 K
Unused 25,108 K 12,604 K 112 K 948 K 11,444 K
Large Page
Total 82,33,204 K 50,26,984 K 26,47,544 K 5,45,884 K 360 K 40 K 948 K 11,444 K
Type here to search
ENG
09:15 AM
16-04-2021
16 April 2021
Friday

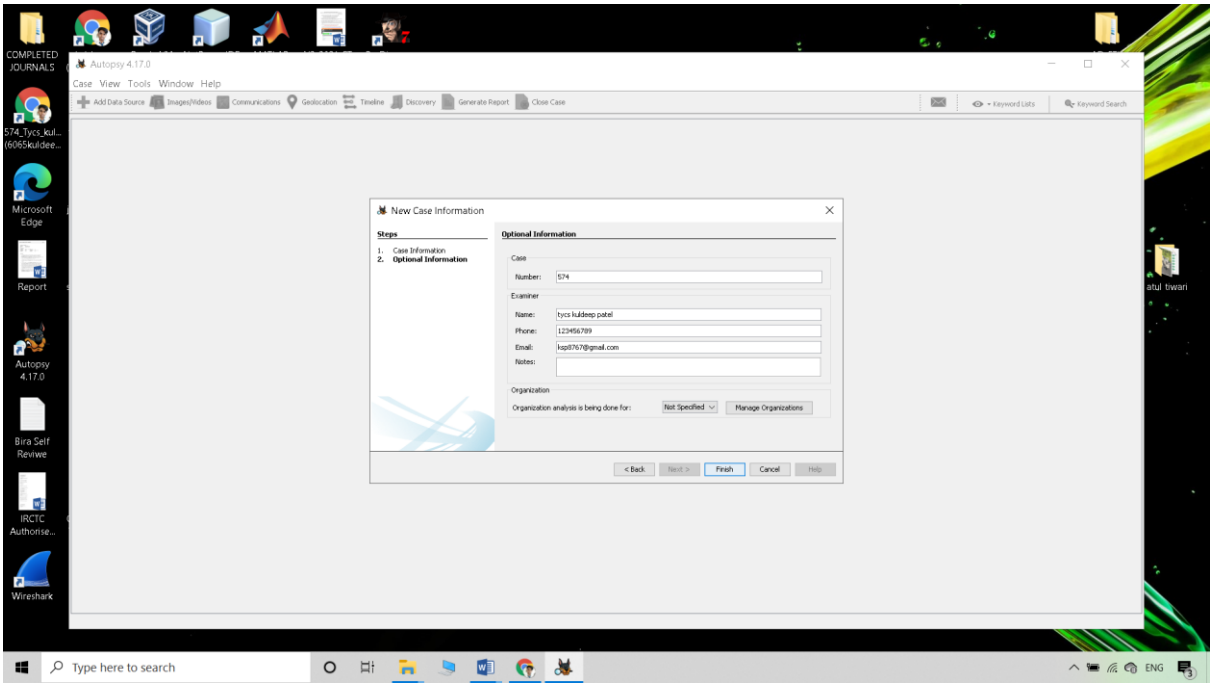
PRACTICAL 7

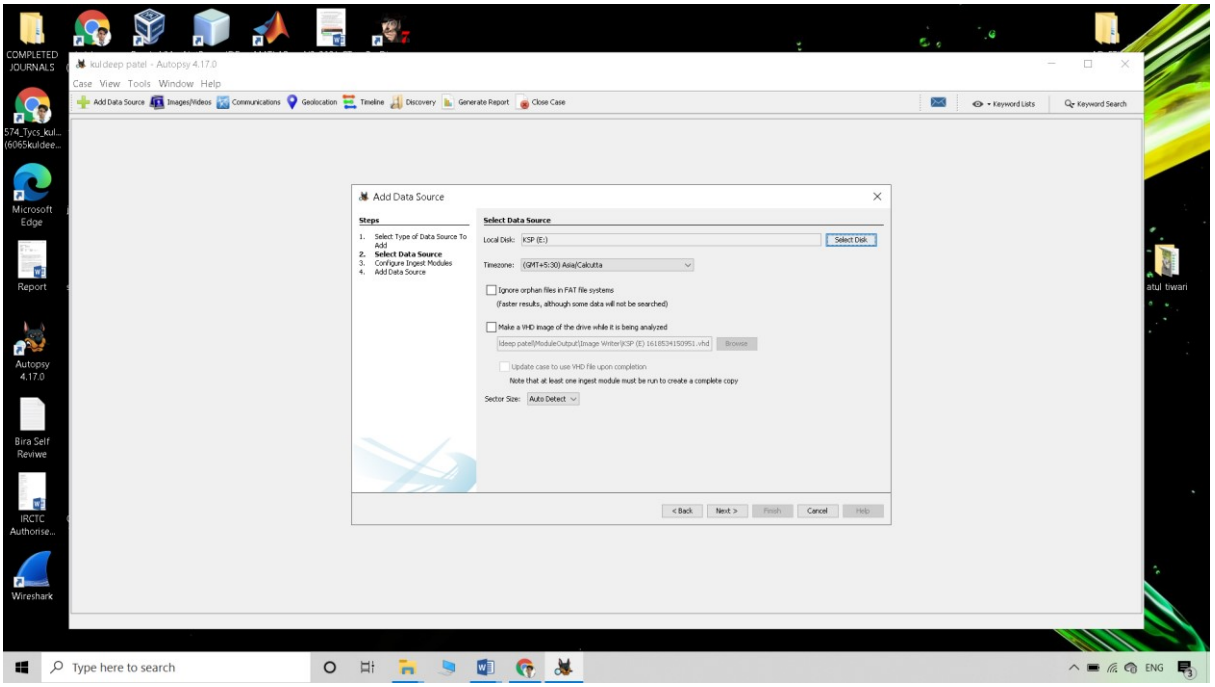
AIM : - Recovering and Inspecting deleted files

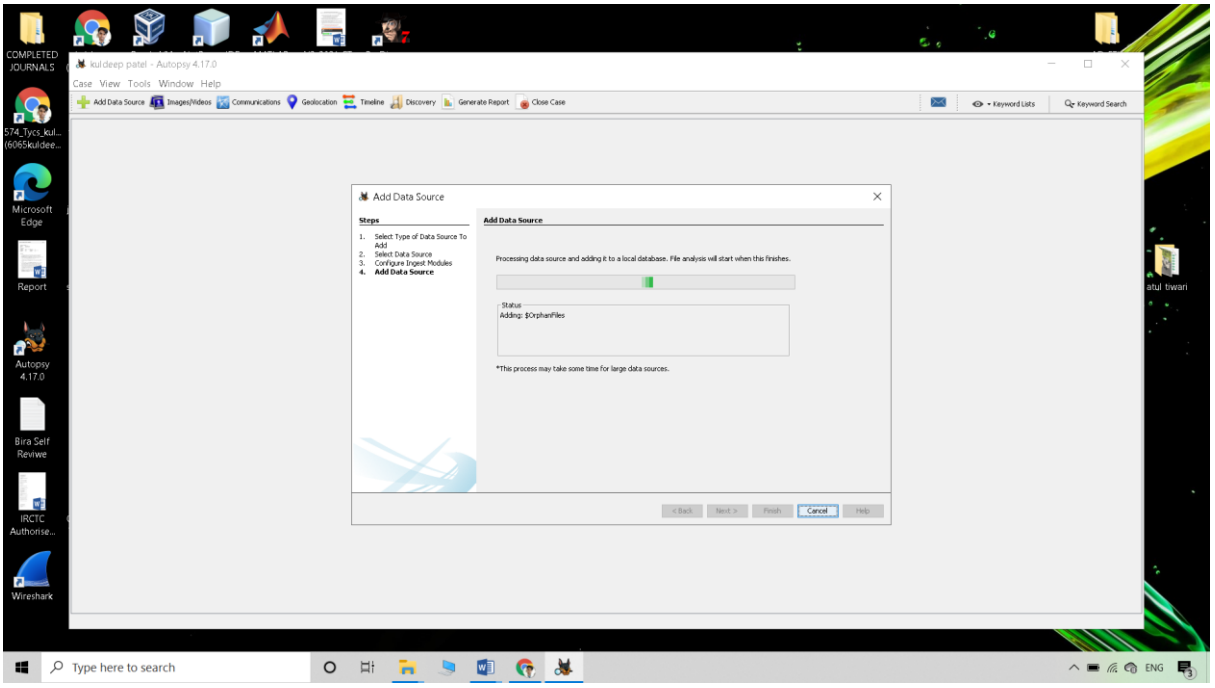
- Check for Deleted Files

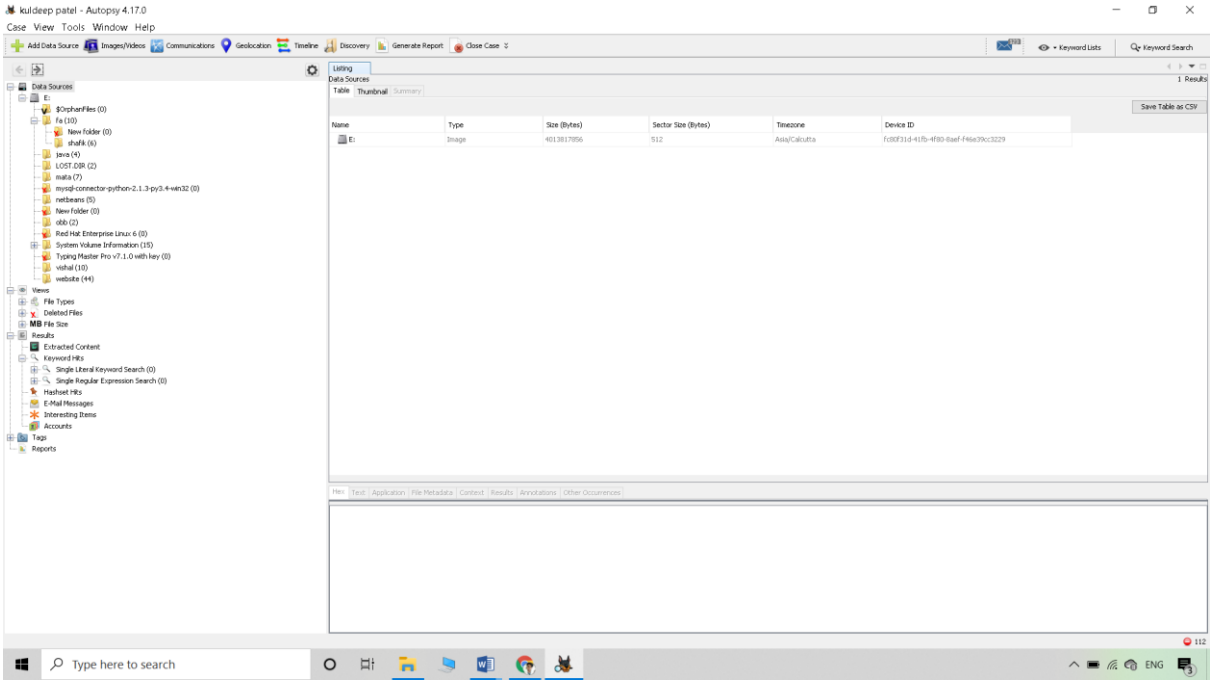
- Recover the Deleted Files

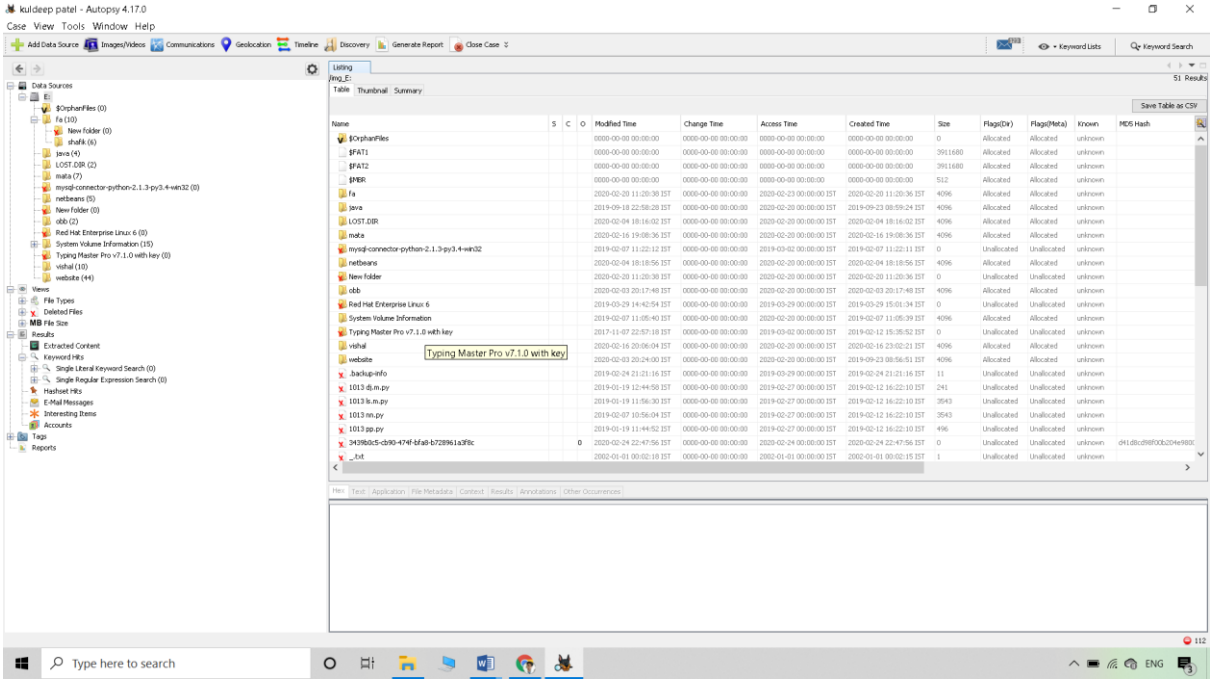
-Analysing and Inspecting the recovered files

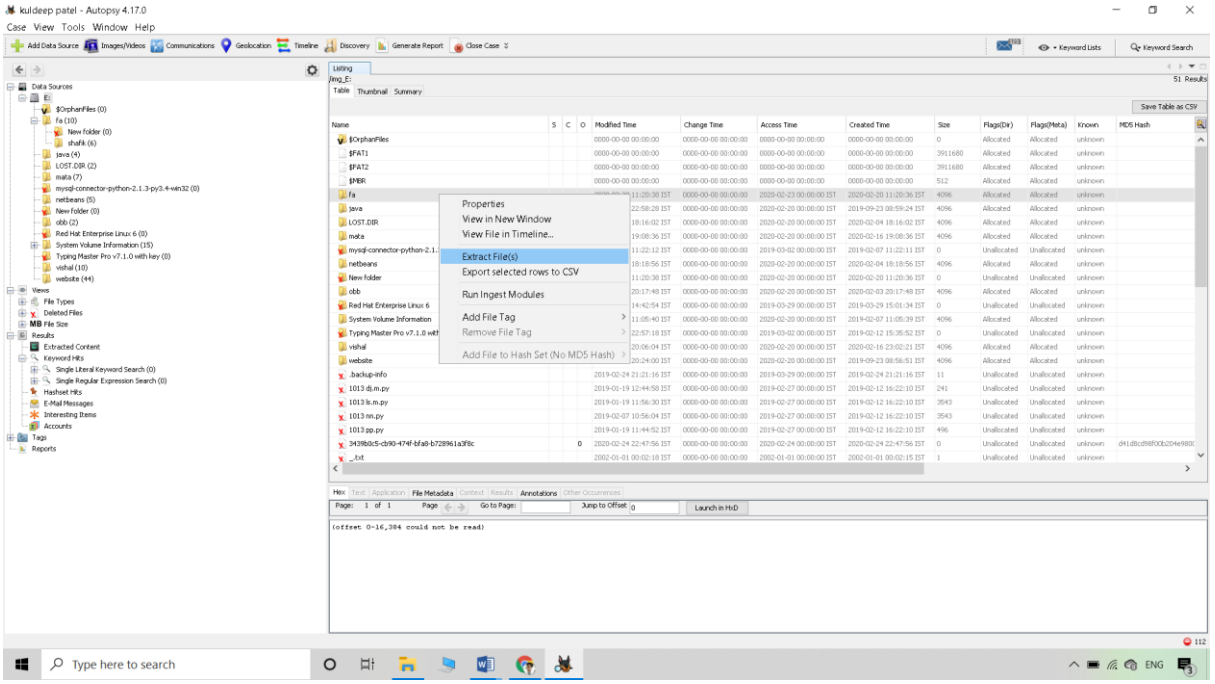


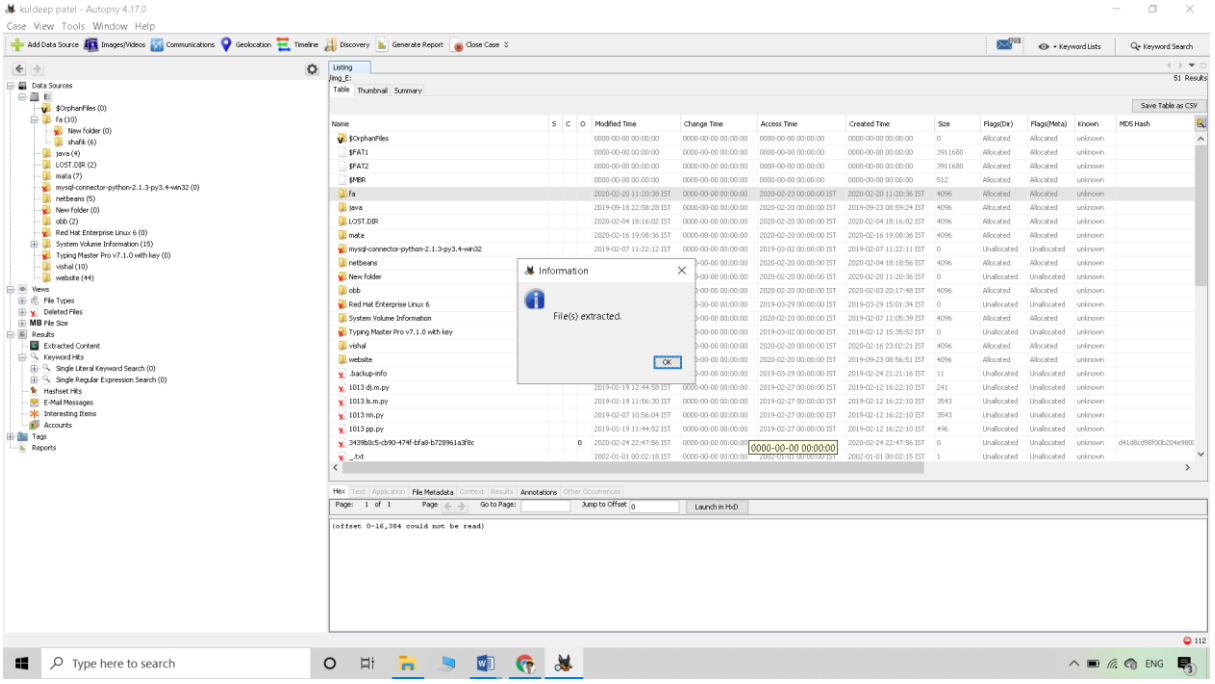

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Local Disk: KSP (E:)
Select Disk
Timezone: (GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
(Faster results, although some data will not be searched)
Make a VHD image of the drive while it is being analyzed
Update case to use VHD file upon completion
Note that at least one ingest module must be run to create a complete copy
Sector Size: Auto Detect
< Back
Next >
Finish
Cancel
Help

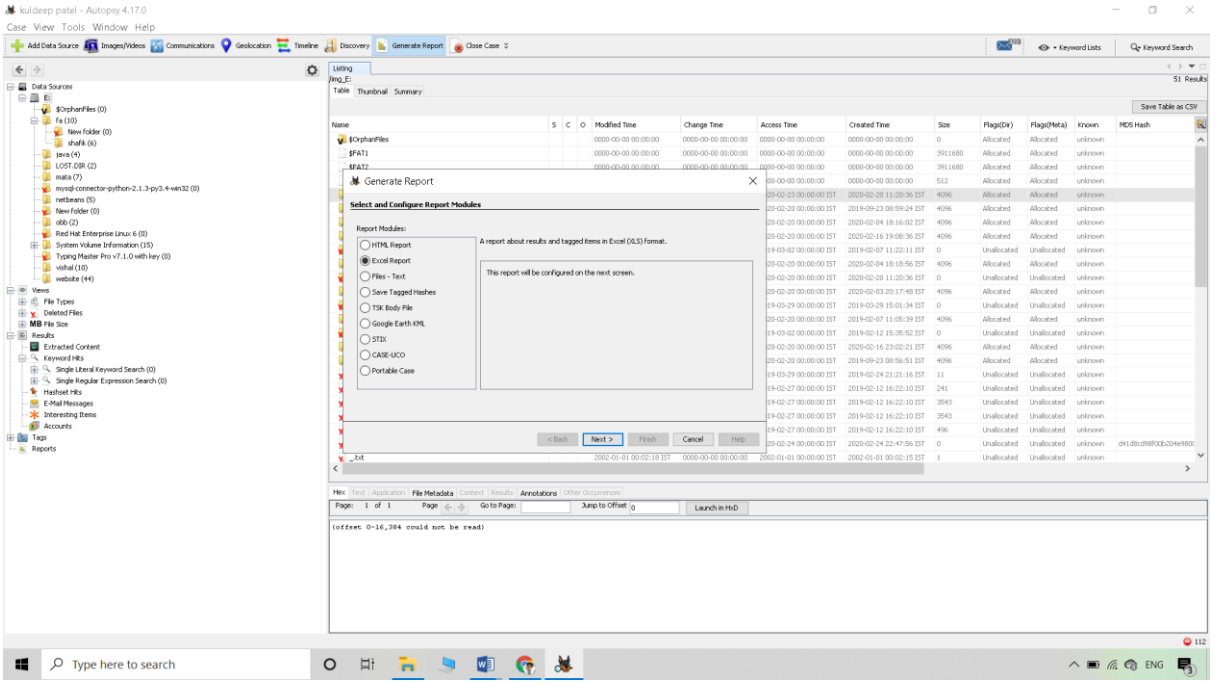

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Add Data Source
Processing data source and adding it to a local database. File analysis will start when this finishes.
Status
Adding: $OrphanFiles
*This process may take some time for large data sources.
< Back
Next >
Finish
Cancel
Help

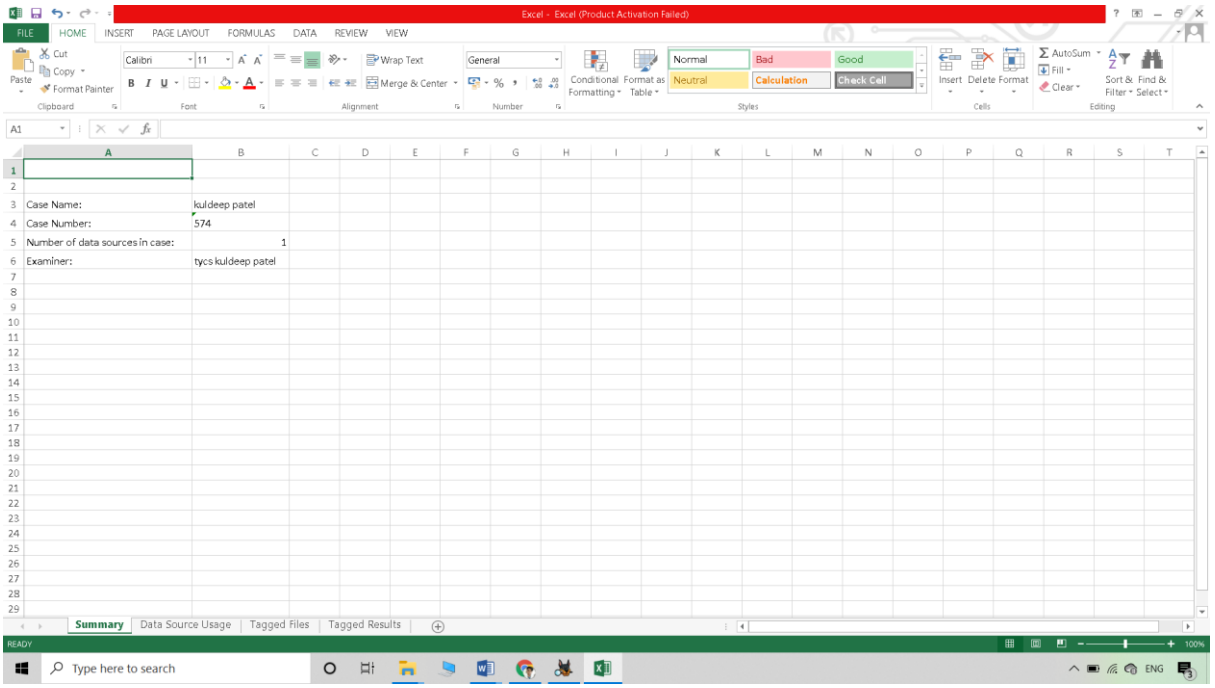

kuldeep patel - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Listing
Table
Thumbnail
Summary
Save Table as CSV
Name
Type
Size (Bytes)
Sector Size (Bytes)
Timezone
Device ID
Type here to search
ENG


kuldeep patel - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Listing
Table
Thumbnail
Summary
Save Table as CSV
Typing Master Pro v7.1.0 with key
Type here to search
ENG


kuldeep patel - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Properties
View in New Window
View File in Timeline...
Extract File(s)
Export selected rows to CSV
Run Ingest Modules
Add File Tag
Remove File Tag
Add File to Hash Set (No MD5 Hash)
(offset 0-16,384 could not be read)
Type here to search
ENG


kuldeep patel - Autopsy 4.17.0
Case View Tools Window Help
Information
File(s) extracted.
OK
(offset 0-16,384 could not be read)
Type here to search
ENG

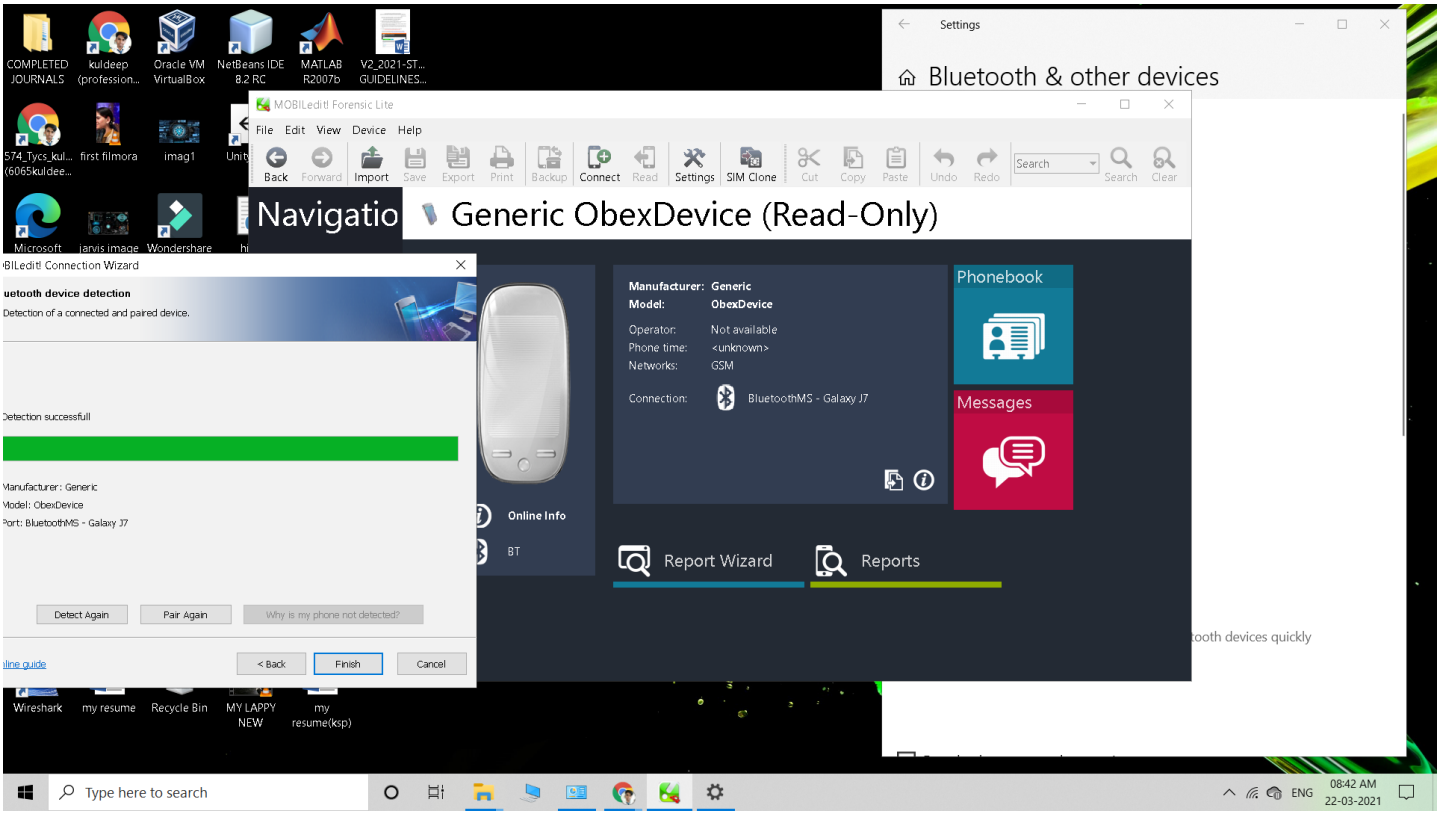

kuldeep patel - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Views
Results
Tags
Reports
Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Save Tagged Hashes
TSK Body File
Google Earth KML
STIX
CASE-UCO
Portable Case
A report about results and tagged items in Excel (XLS) format.
This report will be configured on the next screen.
< Back
Next >
Finish
Cancel
Help
(offset 0-16,384 could not be read)
Type here to search
ENG

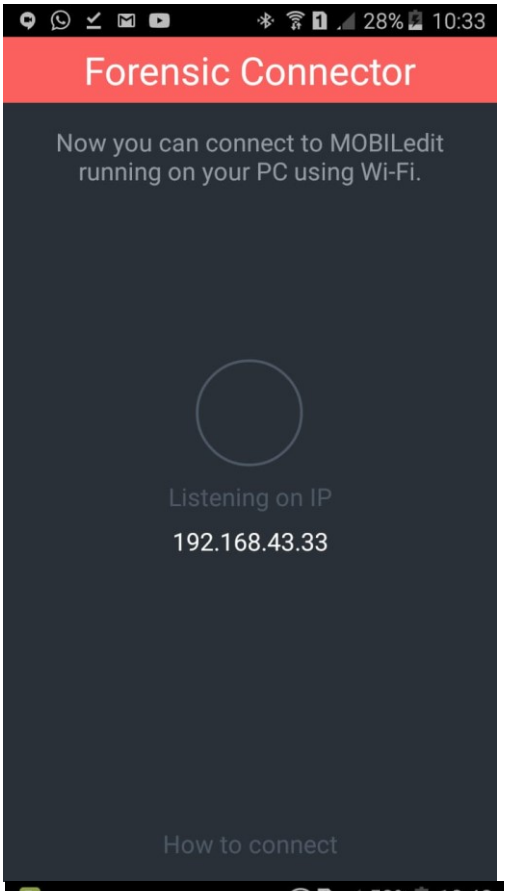

Excel - Excel (Product Activation Failed)
FILE
HOME
INSERT
PAGE LAYOUT
FORMULAS
DATA
REVIEW
VIEW
Paste
Cut
Copy
Format Painter
Clipboard
Calibri
11
Font
Wrap Text
Merge & Center
Alignment
General
Number
Conditional Formatting
Format as Table
Normal
Bad
Good
Neutral
Calculation
Check Cell
Styles
Insert
Delete
Format
Cells
AutoSum
Fill
Clear
Sort & Filter
Find & Select
Editing
A1
Case Name: kuldeep patel
Case Number: 574
Number of data sources in case: 1
Examiner: tycs kuldeep patel
Summary
Data Source Usage
Tagged Files
Tagged Results
READY
Type here to search
ENG

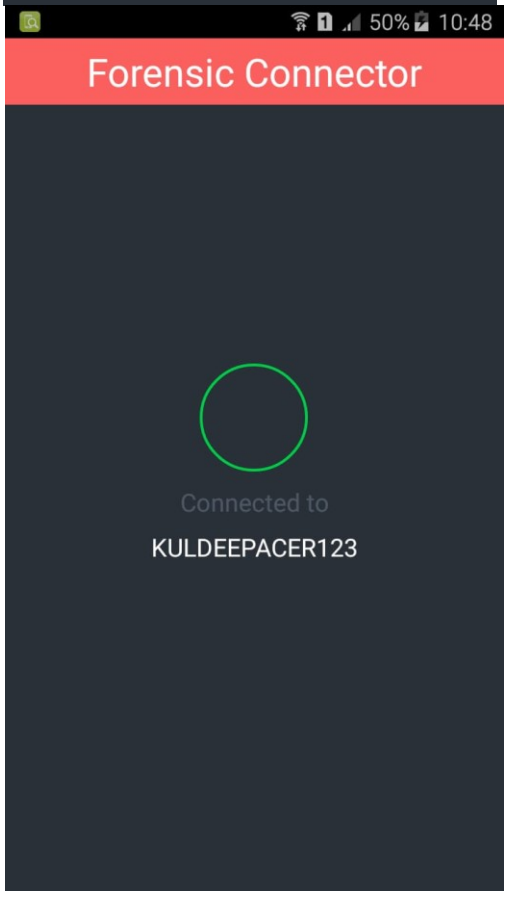
Practical no 8

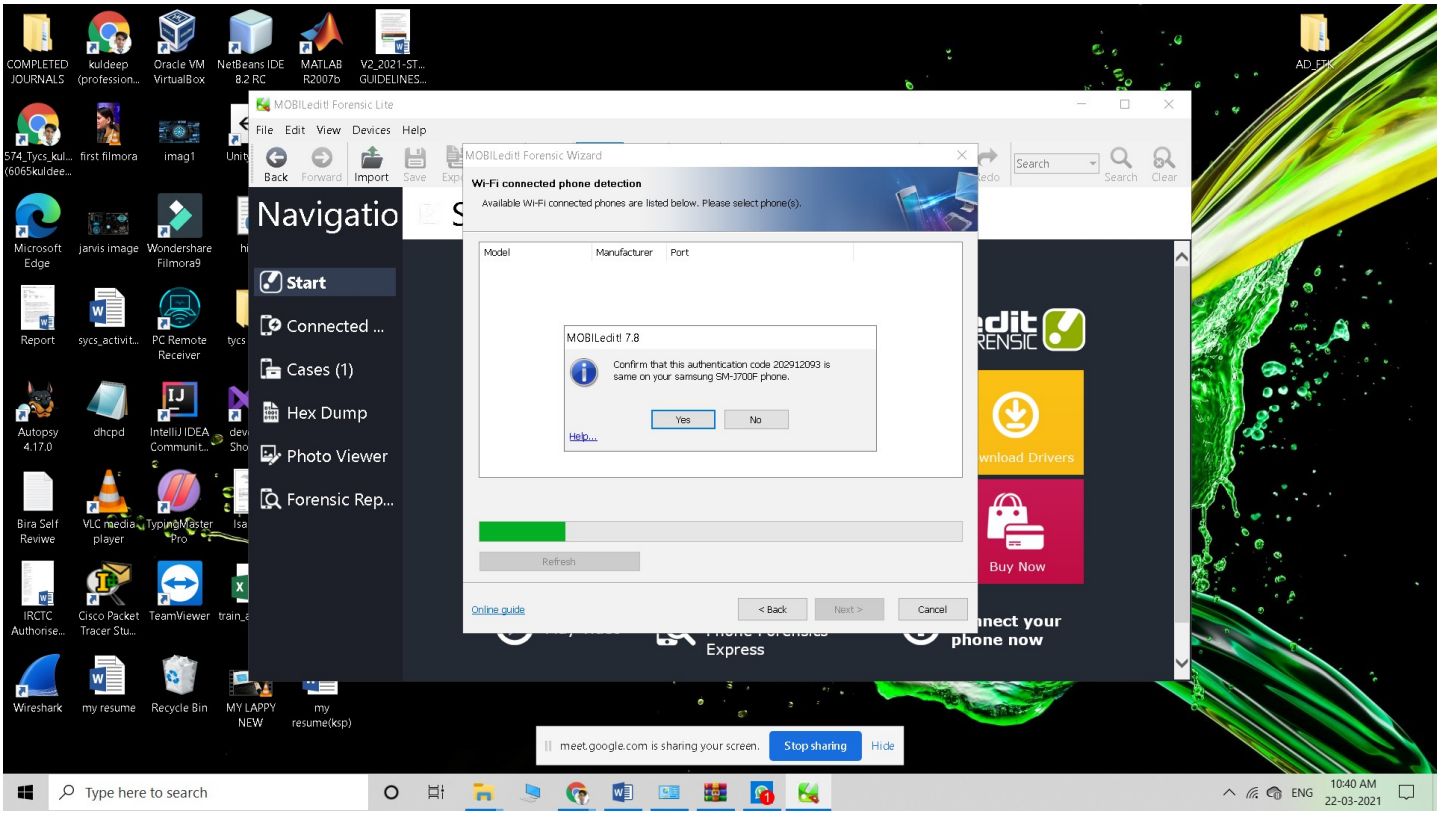
Aim :- Acquisition of Cell phones and Mobile devices .

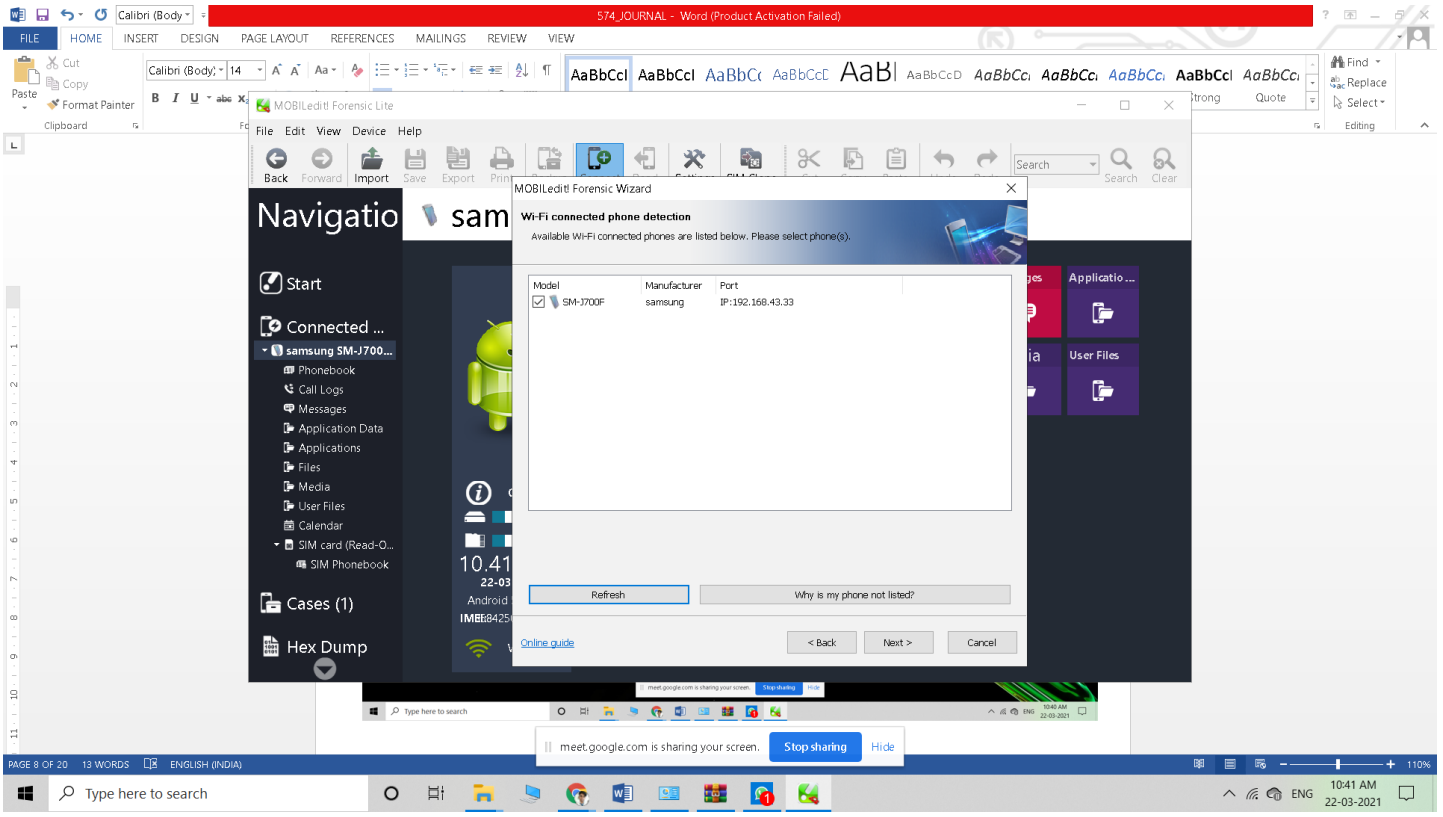
1 : start the application

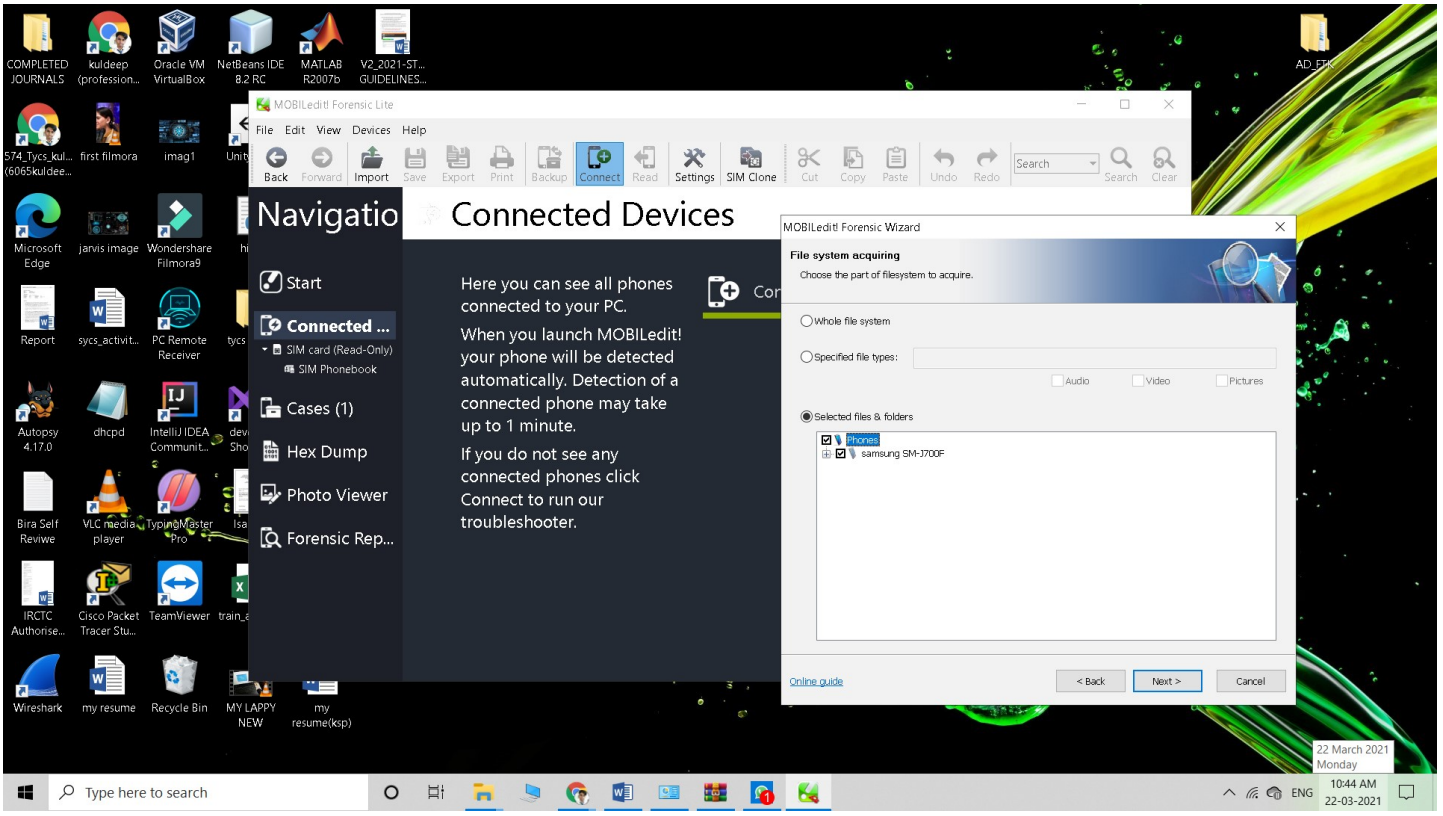


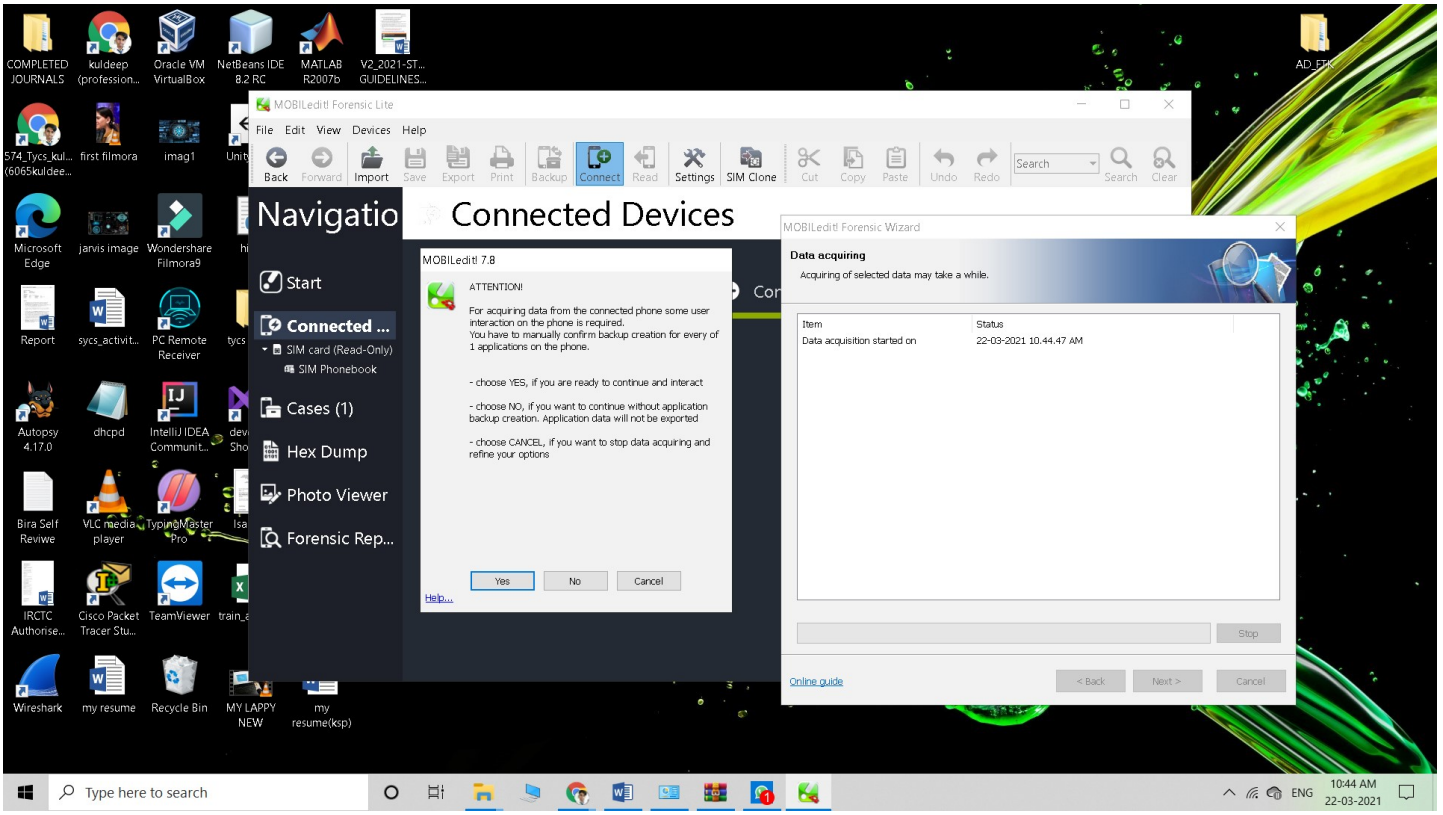

28% 10:33
Forensic Connector
Now you can connect to MOBILedit running on your PC using Wi-Fi.
Listening on IP
192.168.43.33
How to connect

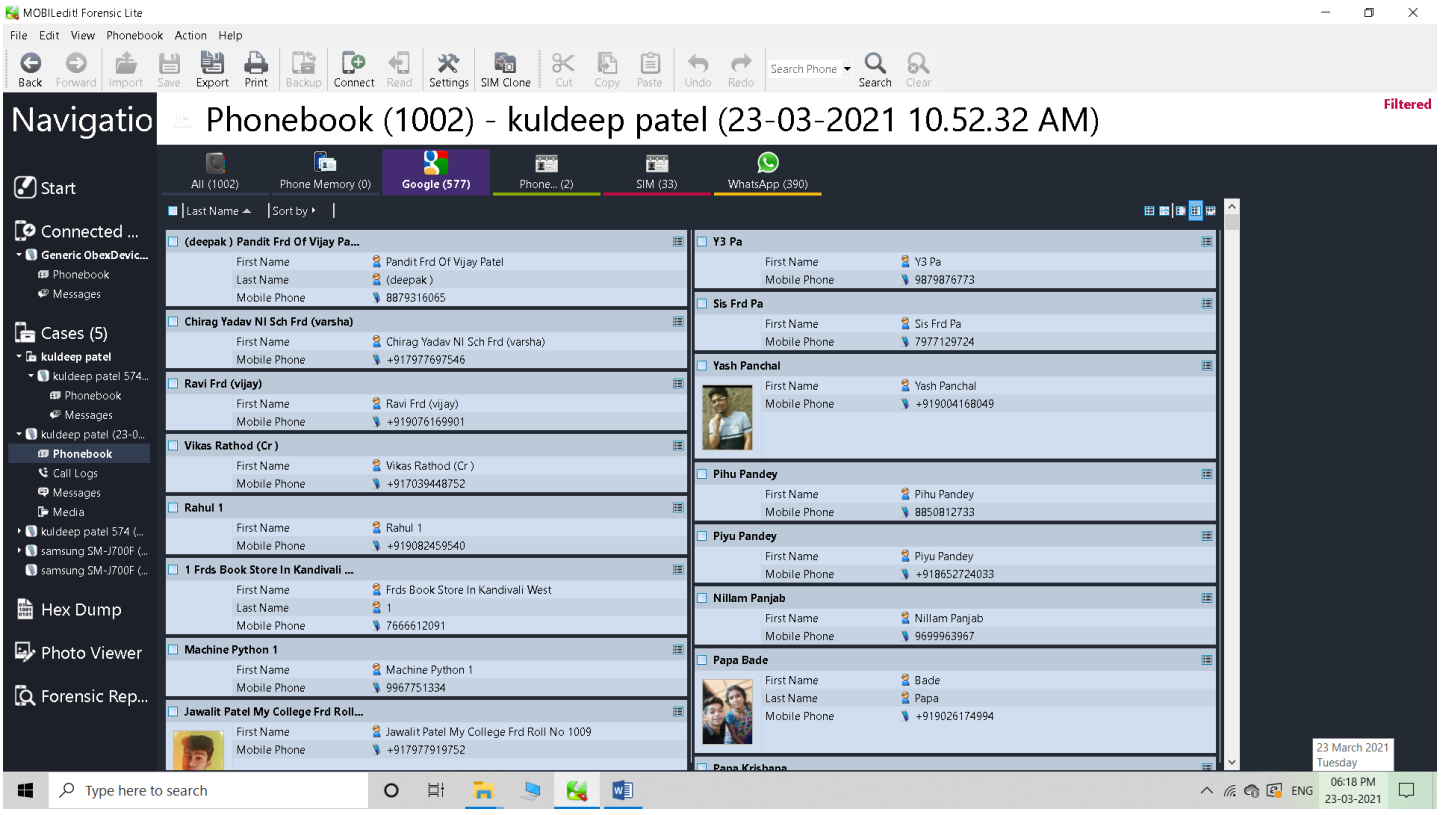

50% 10:48
Forensic Connector
Connected to
KULDEEPACER123

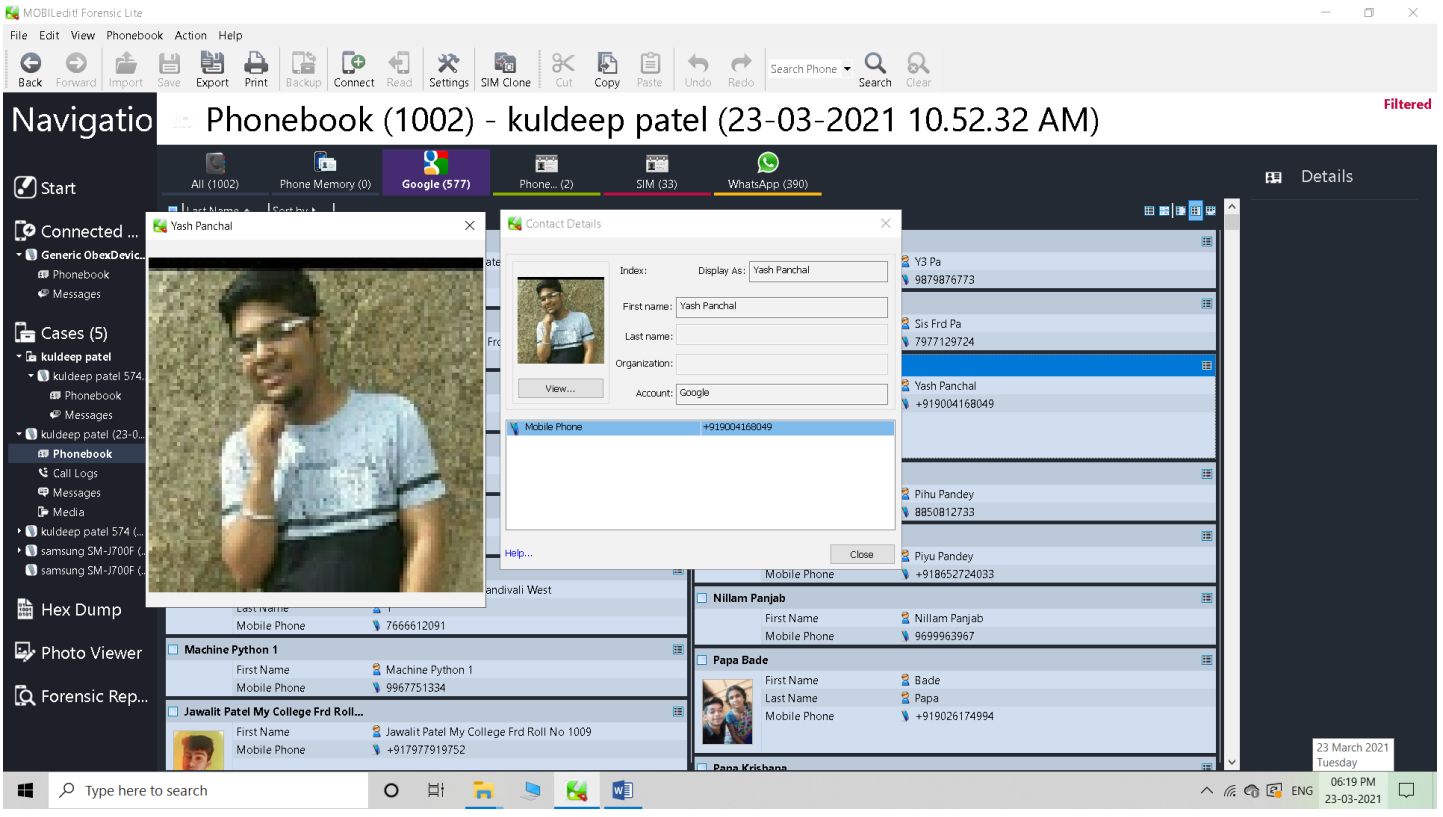

MOBILedit! Forensic Lite
File Edit View Devices Help
Back Forward Import Save
MOBILedit! Forensic Wizard
Wi-Fi connected phone detection
Available Wi-Fi connected phones are listed below. Please select phone(s).
Model Manufacturer Port
MOBILedit! 7.8
Confirm that this authentication code 202912093 is same on your samsung SM-J700F phone.
Yes No
Help...
Refresh
Online guide
< Back Next > Cancel
Navigatio
Start
Connected ...
Cases (1)
Hex Dump
Photo Viewer
Forensic Rep...
Express
Buy Now
meet.google.com is sharing your screen.
Stop sharing
Hide
Type here to search
ENG
10:40 AM
22-03-2021

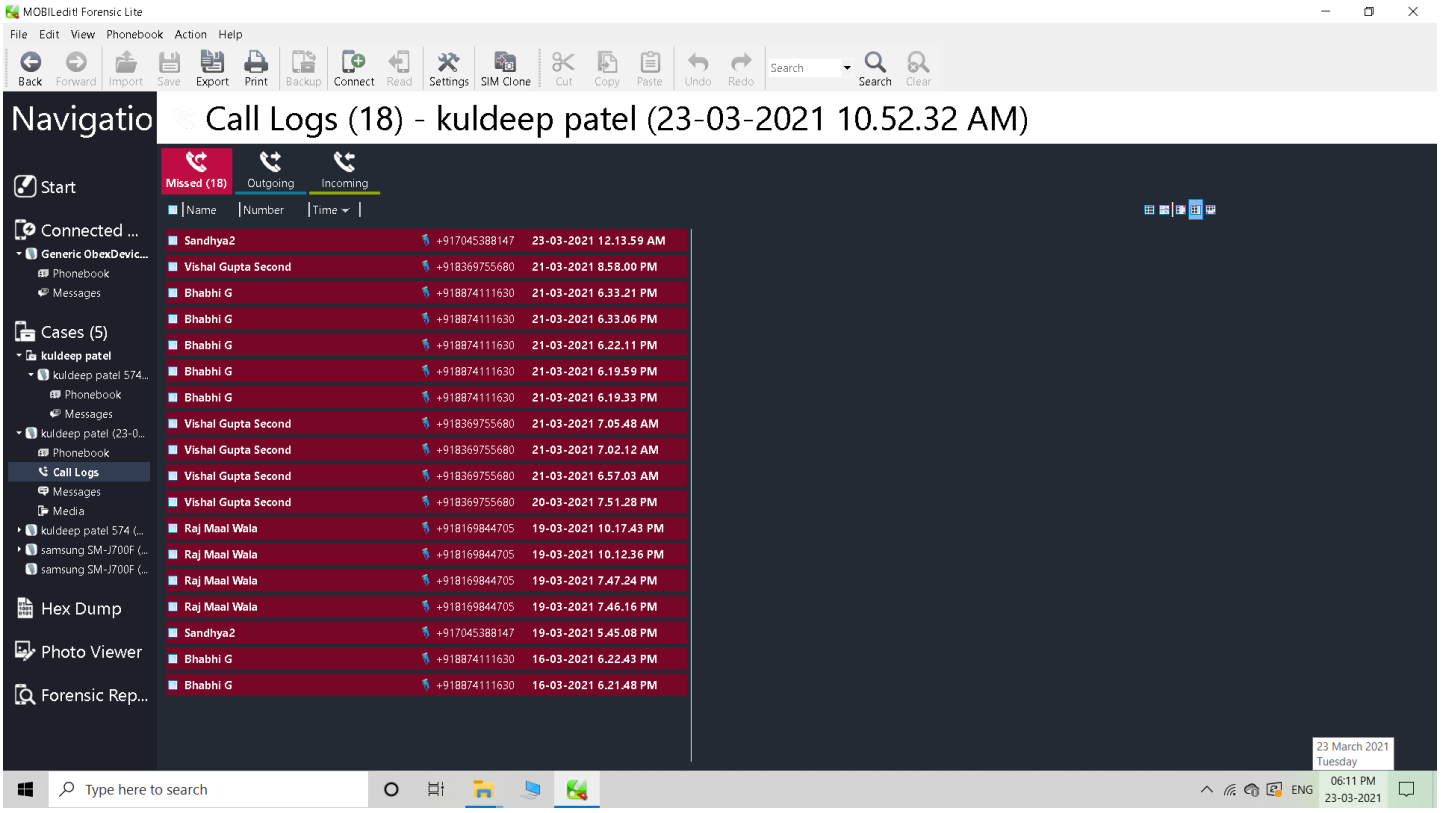

574_JOURNAL - Word (Product Activation Failed)
FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VIEW
MOBILedit! Forensic Lite
File Edit View Device Help
Back Forward Import Save Export
MOBILedit! Forensic Wizard
Wi-Fi connected phone detection
Available Wi-Fi connected phones are listed below. Please select phone(s).
Model Manufacturer Port
SM-J700F samsung IP:192.168.43.33
Refresh
Why is my phone not listed?
Online guide
< Back Next > Cancel
Navigatio
Start
Connected ...
samsung SM-J700...
Phonebook
Call Logs
Messages
Application Data
Applications
Files
Media
User Files
Calendar
SIM card (Read-O...
SIM Phonebook
Cases (1)
Hex Dump
Application ...
User Files
meet.google.com is sharing your screen.
Stop sharing
Hide
PAGE 8 OF 20 13 WORDS ENGLISH (INDIA)
Type here to search
ENG
10:41 AM
22-03-2021

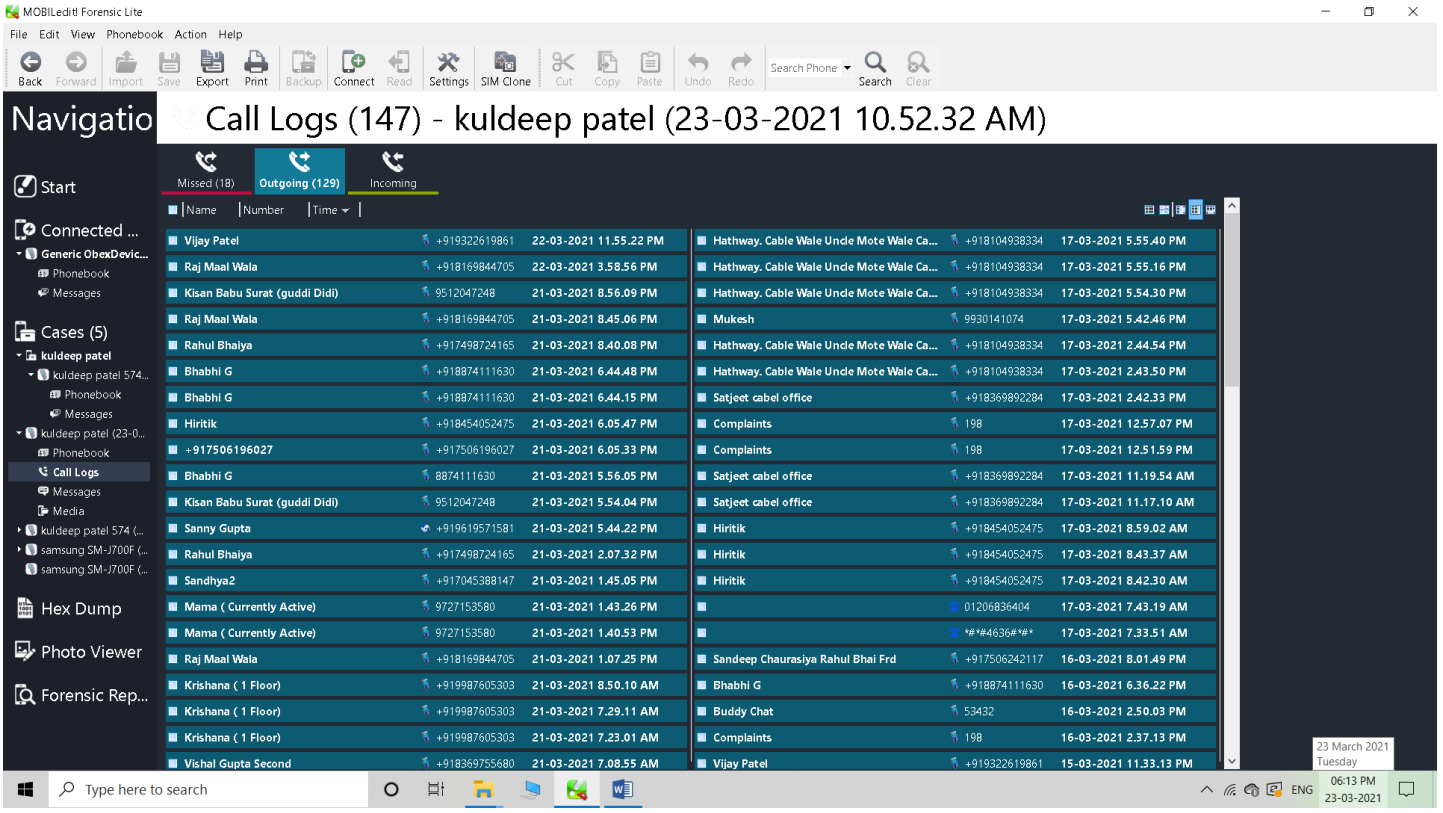

MOBILedit! Forensic Lite
File Edit View Devices Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Search Clear
Navigatio
Connected Devices
Start
Connected ...
SIM card (Read-Only)
SIM Phonebook
Cases (1)
Hex Dump
Photo Viewer
Forensic Rep...
Here you can see all phones connected to your PC.
When you launch MOBILedit! your phone will be detected automatically. Detection of a connected phone may take up to 1 minute.
If you do not see any connected phones click Connect to run our troubleshooter.
MOBILedit! Forensic Wizard
File system acquiring
Choose the part of filesystem to acquire.
Whole file system
Specified file types:
Audio Video Pictures
Selected files & folders
Phones
samsung SM-J700F
Online guide
< Back Next > Cancel
Type here to search
ENG 10:44 AM 22-03-2021

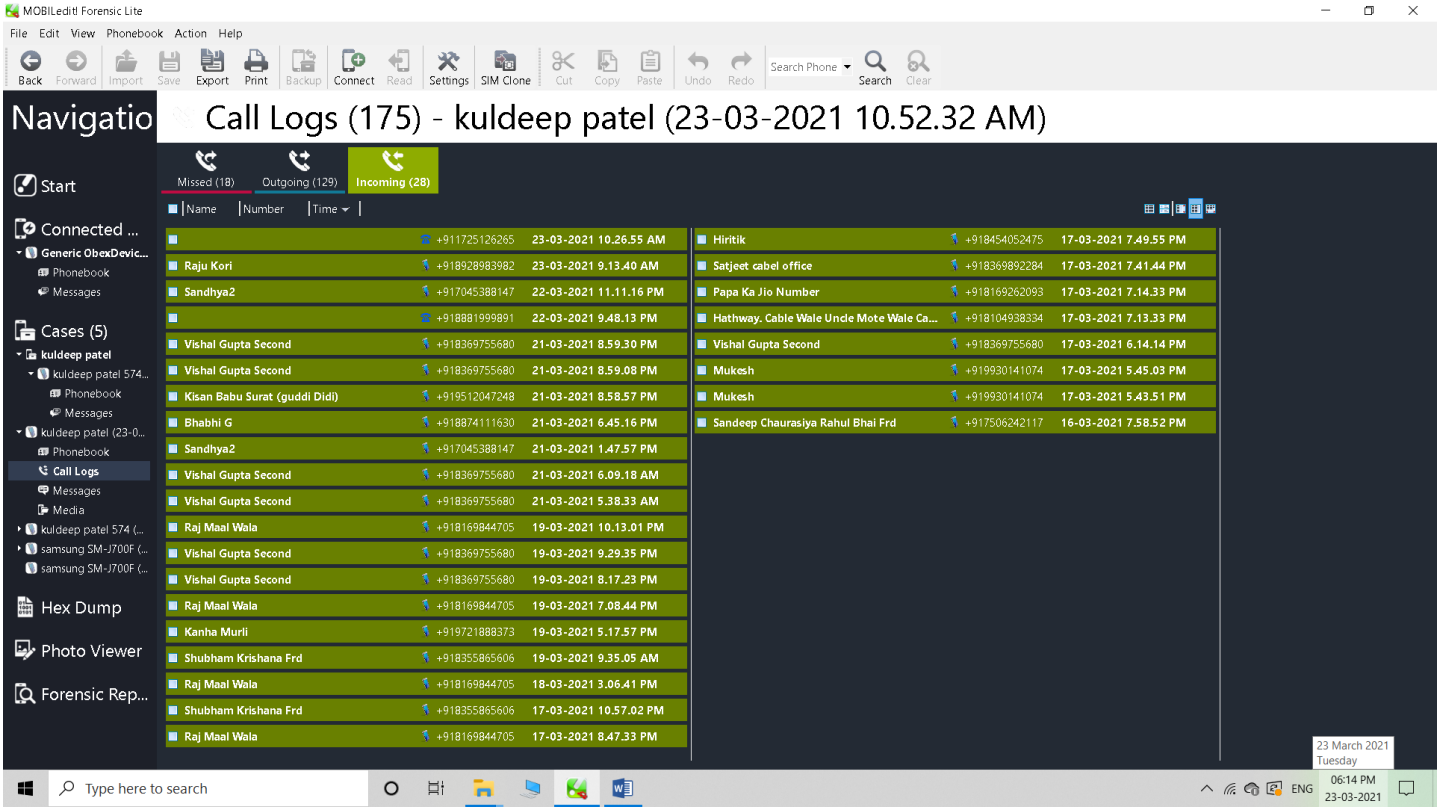

MOBILedit! Forensic Lite
File Edit View Devices Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Search Clear
Navigatio
Connected Devices
Start
Connected ...
SIM card (Read-Only)
SIM Phonebook
Cases (1)
Hex Dump
Photo Viewer
Forensic Rep...
MOBILedit! 7.8
ATTENTION!
For acquiring data from the connected phone some user interaction on the phone is required.
You have to manually confirm backup creation for every of 1 applications on the phone.
- choose YES, if you are ready to continue and interact
- choose NO, if you want to continue without application backup creation. Application data will not be exported
- choose CANCEL, if you want to stop data acquiring and refine your options
Yes No Cancel
Help...
MOBILedit! Forensic Wizard
Data acquiring
Acquiring of selected data may take a while.
Item Status
Data acquisition started on 22-03-2021 10.44.47 AM
Stop
Online guide
< Back Next > Cancel
Type here to search
ENG 10:44 AM 22-03-2021

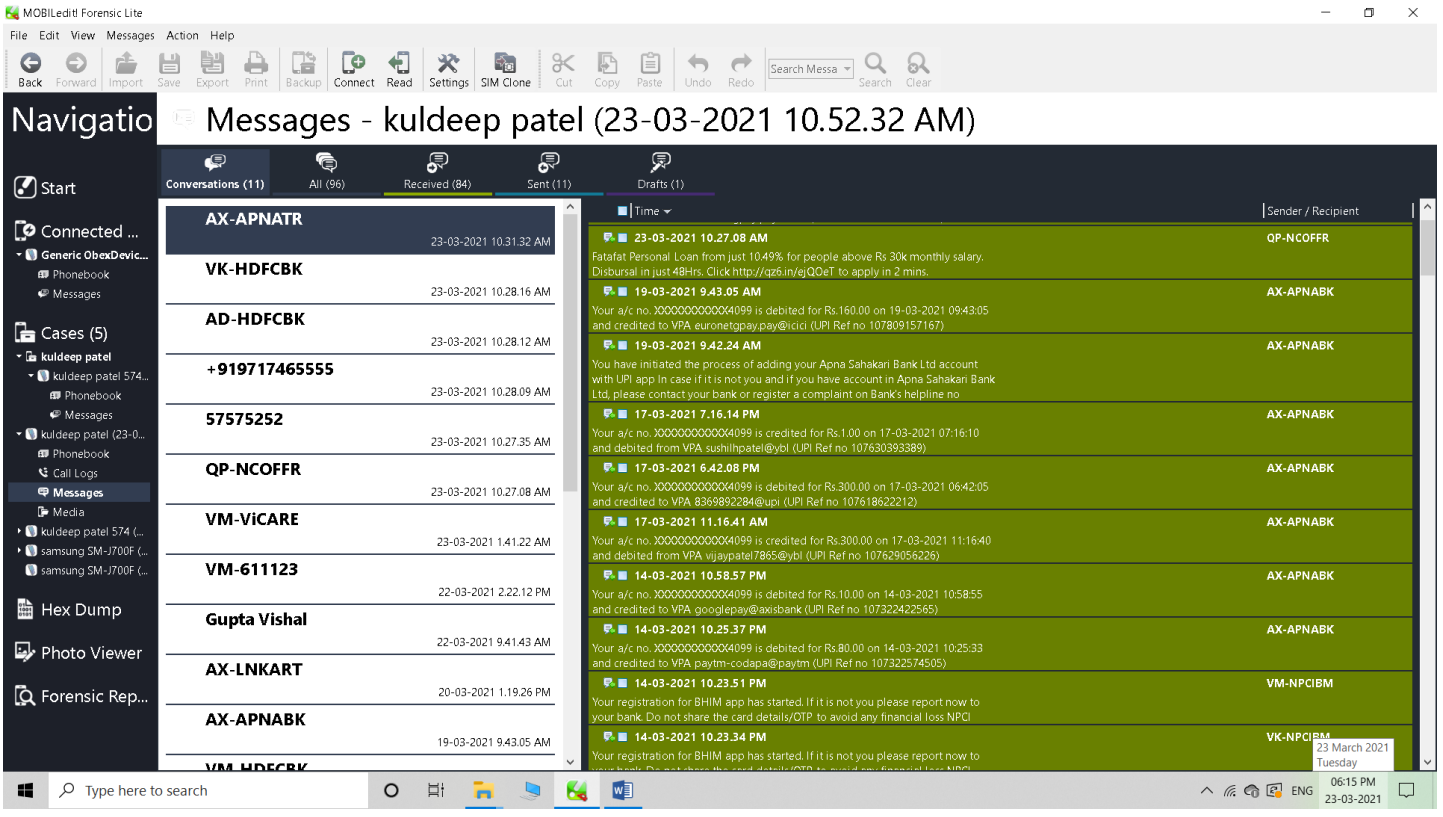

MOBILedit! Forensic Lite
File Edit View Phonebook Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Phone Search Clear
Navigatio
Phonebook (1002) - kuldeep patel (23-03-2021 10.52.32 AM)
Filtered
Start
Connected ...
Generic ObexDevic...
Phonebook
Messages
Cases (5)
kuldeep patel
kuldeep patel 574...
Phonebook
Messages
kuldeep patel (23-0...
Phonebook
Call Logs
Messages
Media
kuldeep patel 574 (...
samsung SM-J700F (...
samsung SM-J700F (...
Hex Dump
Photo Viewer
Forensic Rep...
All (1002)
Phone Memory (0)
Google (577)
Phone... (2)
SIM (33)
WhatsApp (390)
Last Name
Sort by
(deepak) Pandit Frd Of Vijay Pa...
First Name Pandit Frd Of Vijay Patel
Last Name (deepak)
Mobile Phone 8879316065
Chirag Yadav NI Sch Frd (varsha)
First Name Chirag Yadav NI Sch Frd (varsha)
Mobile Phone +917977697546
Ravi Frd (vijay)
First Name Ravi Frd (vijay)
Mobile Phone +919076169901
Vikas Rathod (Cr)
First Name Vikas Rathod (Cr)
Mobile Phone +917039448752
Rahul 1
First Name Rahul 1
Mobile Phone +919082459540
1 Frds Book Store In Kandivali ...
First Name Frds Book Store In Kandivali West
Last Name 1
Mobile Phone 7666612091
Machine Python 1
First Name Machine Python 1
Mobile Phone 9967751334
Jawalit Patel My College Frd Roll...
First Name Jawalit Patel My College Frd Roll No 1009
Mobile Phone +917977919752
Y3 Pa
First Name Y3 Pa
Mobile Phone 9879876773
Sis Frd Pa
First Name Sis Frd Pa
Mobile Phone 7977129724
Yash Panchal
First Name Yash Panchal
Mobile Phone +919004168049
Pihu Pandey
First Name Pihu Pandey
Mobile Phone 8850812733
Piyu Pandey
First Name Piyu Pandey
Mobile Phone +918652724033
Nillam Panjab
First Name Nillam Panjab
Mobile Phone 9699963967
Papa Bade
First Name Bade
Last Name Papa
Mobile Phone +919026174994
23 March 2021
Tuesday
Type here to search
ENG
06:18 PM
23-03-2021

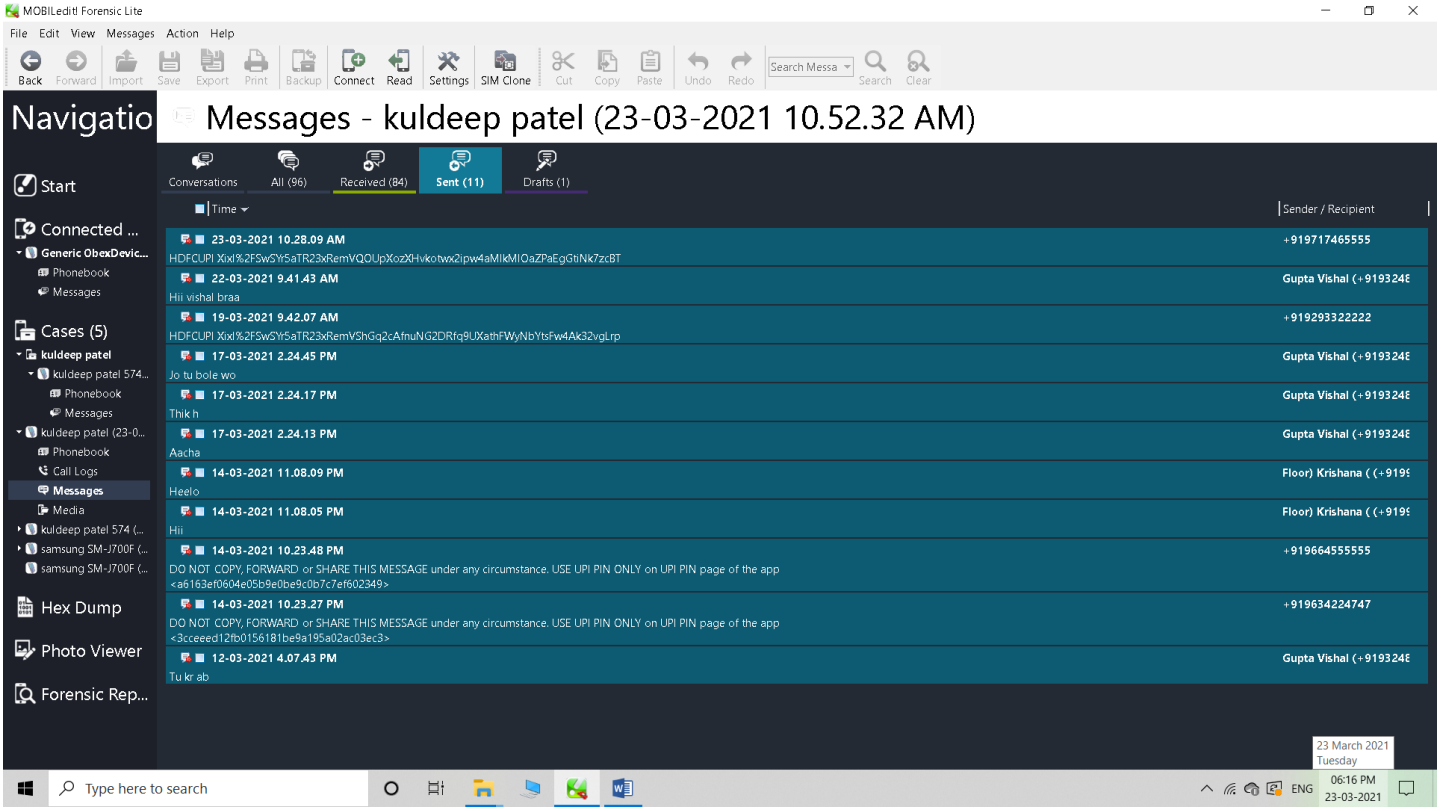

MOBILedit! Forensic Lite
File Edit View Phonebook Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Phone Search Clear
Navigatio
Phonebook (1002) - kuldeep patel (23-03-2021 10.52.32 AM)
Filtered
Details
Yash Panchal
Contact Details
Index:
Display As: Yash Panchal
First name: Yash Panchal
Last name:
Organization:
Account: Google
View...
Mobile Phone +919004168049
Help...
Close
Start
Connected ...
Cases (5)
Hex Dump
Photo Viewer
Forensic Rep...
All (1002)
Phone Memory (0)
Google (577)
Phone... (2)
SIM (33)
WhatsApp (390)
Y3 Pa
9879876773
Sis Frd Pa
7977129724
Yash Panchal
+919004168049
Pihu Pandey
8850812733
Piyu Pandey
Mobile Phone +918652724033
Nillam Panjab
First Name Nillam Panjab
Mobile Phone 9699963967
Papa Bade
First Name Bade
Last Name Papa
Mobile Phone +919026174994
Machine Python 1
First Name Machine Python 1
Mobile Phone 9967751334
Jawalit Patel My College Frd Roll...
First Name Jawalit Patel My College Frd Roll No 1009
Mobile Phone +917977919752
23 March 2021
Tuesday
Type here to search
ENG
06:19 PM
23-03-2021


MOBILedit! Forensic Lite
File Edit View Phonebook Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Clear
Navigatio
Call Logs (18) - kuldeep patel (23-03-2021 10.52.32 AM)
Start
Connected ...
Generic ObexDevic...
Phonebook
Messages
Cases (5)
kuldeep patel
kuldeep patel 574...
Phonebook
Messages
kuldeep patel (23-0...
Phonebook
Call Logs
Messages
Media
kuldeep patel 574 (...
samsung SM-J700F (...
samsung SM-J700F (...
Hex Dump
Photo Viewer
Forensic Rep...
Missed (18)
Outgoing
Incoming
Name
Number
Time
Sandhya2 +917045388147 23-03-2021 12.13.59 AM
Vishal Gupta Second +918369755680 21-03-2021 8.58.00 PM
Bhabhi G +918874111630 21-03-2021 6.33.21 PM
Bhabhi G +918874111630 21-03-2021 6.33.06 PM
Bhabhi G +918874111630 21-03-2021 6.22.11 PM
Bhabhi G +918874111630 21-03-2021 6.19.59 PM
Bhabhi G +918874111630 21-03-2021 6.19.33 PM
Vishal Gupta Second +918369755680 21-03-2021 7.05.48 AM
Vishal Gupta Second +918369755680 21-03-2021 7.02.12 AM
Vishal Gupta Second +918369755680 21-03-2021 6.57.03 AM
Vishal Gupta Second +918369755680 20-03-2021 7.51.28 PM
Raj Maal Wala +918169844705 19-03-2021 10.17.43 PM
Raj Maal Wala +918169844705 19-03-2021 10.12.36 PM
Raj Maal Wala +918169844705 19-03-2021 7.47.24 PM
Raj Maal Wala +918169844705 19-03-2021 7.46.16 PM
Sandhya2 +917045388147 19-03-2021 5.45.08 PM
Bhabhi G +918874111630 16-03-2021 6.22.43 PM
Bhabhi G +918874111630 16-03-2021 6.21.48 PM
23 March 2021
Tuesday
Type here to search
ENG
06:11 PM
23-03-2021


MOBILedit! Forensic Lite
File Edit View Phonebook Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Phone Search Clear
Navigatio
Call Logs (147) - kuldeep patel (23-03-2021 10.52.32 AM)
Start
Connected ...
Generic ObexDevic...
Phonebook
Messages
Cases (5)
kuldeep patel
kuldeep patel 574...
Phonebook
Messages
kuldeep patel (23-0...
Phonebook
Call Logs
Messages
Media
kuldeep patel 574 (...
samsung SM-J700F (...
samsung SM-J700F (...
Hex Dump
Photo Viewer
Forensic Rep...
Missed (18)
Outgoing (129)
Incoming
Name
Number
Time
Vijay Patel +919322619861 22-03-2021 11.55.22 PM
Raj Maal Wala +918169844705 22-03-2021 3.58.56 PM
Kisan Babu Surat (guddi Didi) 9512047248 21-03-2021 8.56.09 PM
Raj Maal Wala +918169844705 21-03-2021 8.45.06 PM
Rahul Bhaiya +917498724165 21-03-2021 8.40.08 PM
Bhabhi G +918874111630 21-03-2021 6.44.48 PM
Bhabhi G +918874111630 21-03-2021 6.44.15 PM
Hiritik +918454052475 21-03-2021 6.05.47 PM
+917506196027 +917506196027 21-03-2021 6.05.33 PM
Bhabhi G 8874111630 21-03-2021 5.56.05 PM
Kisan Babu Surat (guddi Didi) 9512047248 21-03-2021 5.54.04 PM
Sanny Gupta +919619571581 21-03-2021 5.44.22 PM
Rahul Bhaiya +917498724165 21-03-2021 2.07.32 PM
Sandhya2 +917045388147 21-03-2021 1.45.05 PM
Mama (Currently Active) 9727153580 21-03-2021 1.43.26 PM
Mama (Currently Active) 9727153580 21-03-2021 1.40.53 PM
Raj Maal Wala +918169844705 21-03-2021 1.07.25 PM
Krishana (1 Floor) +919987605303 21-03-2021 8.50.10 AM
Krishana (1 Floor) +919987605303 21-03-2021 7.29.11 AM
Krishana (1 Floor) +919987605303 21-03-2021 7.23.01 AM
Vishal Gupta Second +918369755680 21-03-2021 7.08.55 AM
Hathway. Cable Wale Uncle Mote Wale Ca... +918104938334 17-03-2021 5.55.40 PM
Hathway. Cable Wale Uncle Mote Wale Ca... +918104938334 17-03-2021 5.55.16 PM
Hathway. Cable Wale Uncle Mote Wale Ca... +918104938334 17-03-2021 5.54.30 PM
Mukesh 9930141074 17-03-2021 5.42.46 PM
Hathway. Cable Wale Uncle Mote Wale Ca... +918104938334 17-03-2021 2.44.54 PM
Hathway. Cable Wale Uncle Mote Wale Ca... +918104938334 17-03-2021 2.43.50 PM
Satjeet cabel office +918369892284 17-03-2021 2.42.33 PM
Complaints 198 17-03-2021 12.57.07 PM
Complaints 198 17-03-2021 12.51.59 PM
Satjeet cabel office +918369892284 17-03-2021 11.19.54 AM
Satjeet cabel office +918369892284 17-03-2021 11.17.10 AM
Hiritik +918454052475 17-03-2021 8.59.02 AM
Hiritik +918454052475 17-03-2021 8.43.37 AM
Hiritik +918454052475 17-03-2021 8.42.30 AM
01206836404 17-03-2021 7.43.19 AM
##4636#*#* 17-03-2021 7.33.51 AM
Sandeep Chaurasiya Rahul Bhai Frd +917506242117 16-03-2021 8.01.49 PM
Bhabhi G +918874111630 16-03-2021 6.36.22 PM
Buddy Chat 53432 16-03-2021 2.50.03 PM
Complaints 198 16-03-2021 2.37.13 PM
Vijay Patel +919322619861 15-03-2021 11.33.13 PM
23 March 2021
Tuesday
Type here to search
ENG
06:13 PM
23-03-2021


MOBILedit! Forensic Lite
File Edit View Phonebook Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Phone Search Clear
Navigatio
Call Logs (175) - kuldeep patel (23-03-2021 10.52.32 AM)
Start
Connected ...
Generic ObexDevic...
Phonebook
Messages
Cases (5)
kuldeep patel
kuldeep patel 574...
Phonebook
Messages
kuldeep patel (23-0...
Phonebook
Call Logs
Messages
Media
kuldeep patel 574 (...
samsung SM-J700F (...
samsung SM-J700F (...
Hex Dump
Photo Viewer
Forensic Rep...
Missed (18)
Outgoing (129)
Incoming (28)
Name
Number
Time
+911725126265 23-03-2021 10.26.55 AM
Raju Kori +918928983982 23-03-2021 9.13.40 AM
Sandhya2 +917045388147 22-03-2021 11.11.16 PM
+918881999891 22-03-2021 9.48.13 PM
Vishal Gupta Second +918369755680 21-03-2021 8.59.30 PM
Vishal Gupta Second +918369755680 21-03-2021 8.59.08 PM
Kisan Babu Surat (guddi Didi) +919512047248 21-03-2021 8.58.57 PM
Bhabhi G +918874111630 21-03-2021 6.45.16 PM
Sandhya2 +917045388147 21-03-2021 1.47.57 PM
Vishal Gupta Second +918369755680 21-03-2021 6.09.18 AM
Vishal Gupta Second +918369755680 21-03-2021 5.38.33 AM
Raj Maal Wala +918169844705 19-03-2021 10.13.01 PM
Vishal Gupta Second +918369755680 19-03-2021 9.29.35 PM
Vishal Gupta Second +918369755680 19-03-2021 8.17.23 PM
Raj Maal Wala +918169844705 19-03-2021 7.08.44 PM
Kanha Murli +919721888373 19-03-2021 5.17.57 PM
Shubham Krishana Frd +918355865606 19-03-2021 9.35.05 AM
Raj Maal Wala +918169844705 18-03-2021 3.06.41 PM
Shubham Krishana Frd +918355865606 17-03-2021 10.57.02 PM
Raj Maal Wala +918169844705 17-03-2021 8.47.33 PM
Hiritik +918454052475 17-03-2021 7.49.55 PM
Satjeet cabel office +918369892284 17-03-2021 7.41.44 PM
Papa Ka Jio Number +918169262093 17-03-2021 7.14.33 PM
Hathway. Cable Wale Uncle Mote Wale Ca... +918104938334 17-03-2021 7.13.33 PM
Vishal Gupta Second +918369755680 17-03-2021 6.14.14 PM
Mukesh +919930141074 17-03-2021 5.45.03 PM
Mukesh +919930141074 17-03-2021 5.43.51 PM
Sandeep Chaurasiya Rahul Bhai Frd +917506242117 16-03-2021 7.58.52 PM
23 March 2021 Tuesday
Type here to search
ENG 06:14 PM 23-03-2021


MOBILedit! Forensic Lite
File Edit View Messages Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Messa Search Clear
Navigatio
Messages - kuldeep patel (23-03-2021 10.52.32 AM)
Start
Connected ...
Generic ObexDevic...
Phonebook
Messages
Cases (5)
kuldeep patel
kuldeep patel 574...
Phonebook
Messages
kuldeep patel (23-0...
Phonebook
Call Logs
Messages
Media
kuldeep patel 574 (...
samsung SM-J700F (...
samsung SM-J700F (...
Hex Dump
Photo Viewer
Forensic Rep...
Conversations (11)
All (96)
Received (84)
Sent (11)
Drafts (1)
AX-APNATR 23-03-2021 10.31.32 AM
VK-HDFCBK 23-03-2021 10.28.16 AM
AD-HDFCBK 23-03-2021 10.28.12 AM
+919717465555 23-03-2021 10.28.09 AM
57575252 23-03-2021 10.27.35 AM
QP-NCOFFR 23-03-2021 10.27.08 AM
VM-ViCARE 23-03-2021 1.41.22 AM
VM-611123 22-03-2021 2.22.12 PM
Gupta Vishal 22-03-2021 9.41.43 AM
AX-LNKART 20-03-2021 1.19.26 PM
AX-APNABK 19-03-2021 9.43.05 AM
Time
Sender / Recipient
23-03-2021 10.27.08 AM QP-NCOFFR
Fatafat Personal Loan from just 10.49% for people above Rs 30k monthly salary. Disbursal in just 48Hrs. Click http://qz6.in/ejQOeT to apply in 2 mins.
19-03-2021 9.43.05 AM AX-APNABK
Your a/c no. XXXXXXXXXX4099 is debited for Rs.160.00 on 19-03-2021 09:43:05 and credited to VPA euronetgpay.pay@icici (UPI Ref no 107809157167)
19-03-2021 9.42.24 AM AX-APNABK
You have initiated the process of adding your Apna Sahakari Bank Ltd account with UPI app In case if it is not you and if you have account in Apna Sahakari Bank Ltd, please contact your bank or register a complaint on Bank's helpline no
17-03-2021 7.16.14 PM AX-APNABK
Your a/c no. XXXXXXXXXX4099 is credited for Rs.1.00 on 17-03-2021 07:16:10 and debited from VPA sushilhpatel@ybl (UPI Ref no 107630393389)
17-03-2021 6.42.08 PM AX-APNABK
Your a/c no. XXXXXXXXXX4099 is debited for Rs.300.00 on 17-03-2021 06:42:05 and credited to VPA 8369892284@upi (UPI Ref no 107618622212)
17-03-2021 11.16.41 AM AX-APNABK
Your a/c no. XXXXXXXXXX4099 is credited for Rs.300.00 on 17-03-2021 11:16:40 and debited from VPA vijaypatel7865@ybl (UPI Ref no 107629056226)
14-03-2021 10.58.57 PM AX-APNABK
Your a/c no. XXXXXXXXXX4099 is debited for Rs.10.00 on 14-03-2021 10:58:55 and credited to VPA googlepay@axisbank (UPI Ref no 107322422565)
14-03-2021 10.25.37 PM AX-APNABK
Your a/c no. XXXXXXXXXX4099 is debited for Rs.80.00 on 14-03-2021 10:25:33 and credited to VPA paytm-codapa@paytm (UPI Ref no 107322574505)
14-03-2021 10.23.51 PM VM-NPCIBM
Your registration for BHIM app has started. If it is not you please report now to your bank. Do not share the card details/OTP to avoid any financial loss NPCI
14-03-2021 10.23.34 PM VK-NPCIBM
Your registration for BHIM app has started. If it is not you please report now to
23 March 2021 Tuesday
Type here to search
ENG 06:15 PM 23-03-2021


MOBILedit! Forensic Lite
File Edit View Messages Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Search Clear
Navigatio
Messages - kuldeep patel (23-03-2021 10.52.32 AM)
Start
Connected ...
Generic ObexDevic...
Phonebook
Messages
Cases (5)
kuldeep patel
kuldeep patel 574...
Phonebook
Messages
kuldeep patel (23-0...
Phonebook
Call Logs
Messages
Media
kuldeep patel 574 (...
samsung SM-J700F (...
samsung SM-J700F (...
Hex Dump
Photo Viewer
Forensic Rep...
Conversations
All (96)
Received (84)
Sent (11)
Drafts (1)
Time
Sender / Recipient
23-03-2021 10.28.09 AM
+919717465555
HDFCUPI Xixl%2FSwSYr5aTR23xRemVQOUpXozGHvkotwx2ipw4aMIkMIOaZPaEgGtiNk7zcBT
22-03-2021 9.41.43 AM
Gupta Vishal (+919324E
Hii vishal braa
19-03-2021 9.42.07 AM
+919293322222
HDFCUPI Xixl%2FSwSYr5aTR23xRemVShGq2cAfnuNG2DRfq9UXathFWyNbYtsFw4Ak32vgLrp
17-03-2021 2.24.45 PM
Gupta Vishal (+919324E
Jo tu bole wo
17-03-2021 2.24.17 PM
Gupta Vishal (+919324E
Thik h
17-03-2021 2.24.13 PM
Gupta Vishal (+919324E
Aacha
14-03-2021 11.08.09 PM
Floor) Krishana ((+919
Heelo
14-03-2021 11.08.05 PM
Floor) Krishana ((+919
Hii
14-03-2021 10.23.48 PM
+919664555555
DO NOT COPY, FORWARD or SHARE THIS MESSAGE under any circumstance. USE UPI PIN ONLY on UPI PIN page of the app
<a6163ef0604e05b9e0be9c0b7c7ef602349>
14-03-2021 10.23.27 PM
+919634224747
DO NOT COPY, FORWARD or SHARE THIS MESSAGE under any circumstance. USE UPI PIN ONLY on UPI PIN page of the app
<3cceeed12fb0156181be9a195a02ac03ec3>
12-03-2021 4.07.43 PM
Gupta Vishal (+919324E
Tu kr ab
23 March 2021
Tuesday
Type here to search
ENG
06:16 PM
23-03-2021

Practical no 9

Aim:- Email Forensics

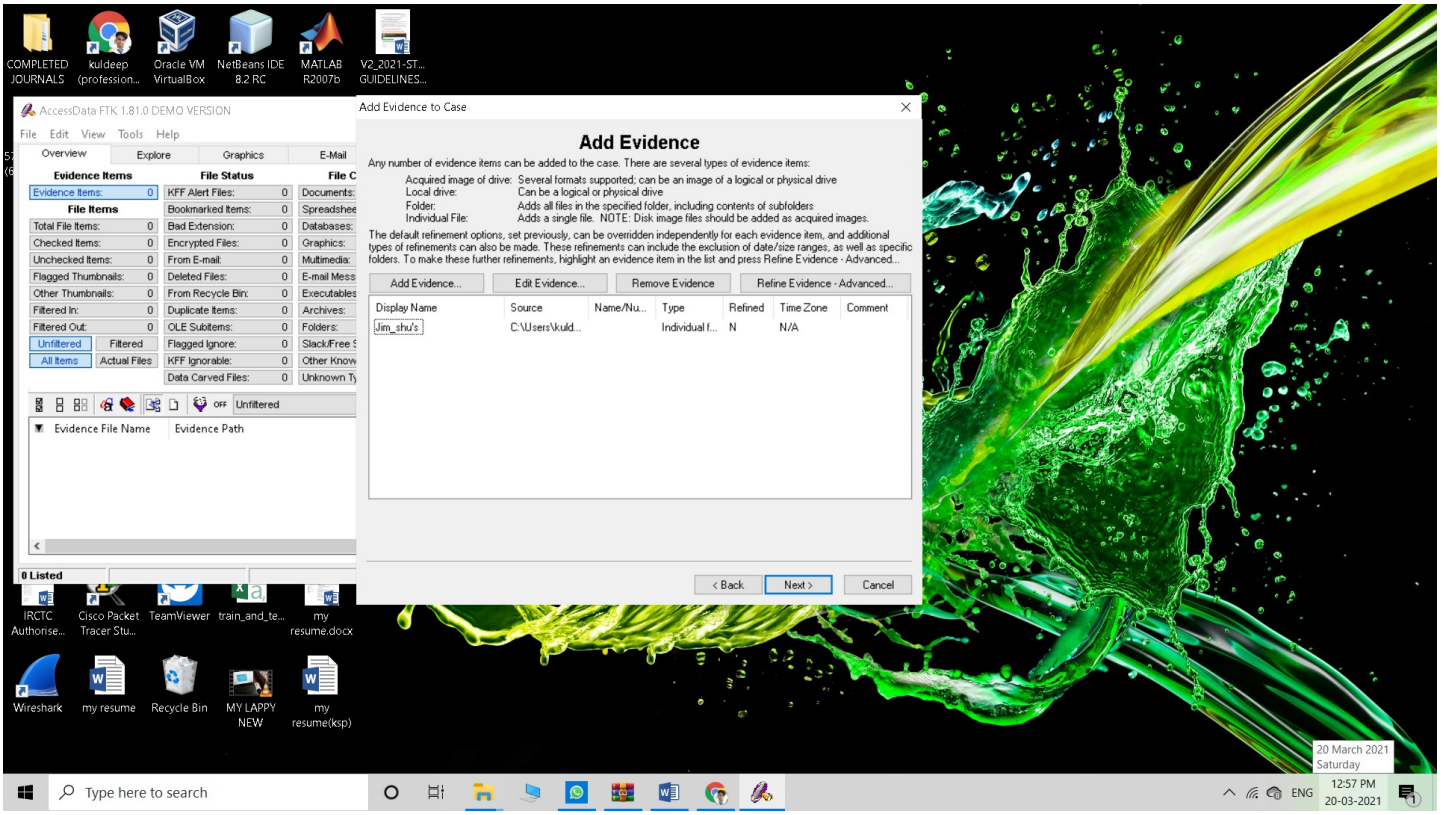
- Mail Service Providers

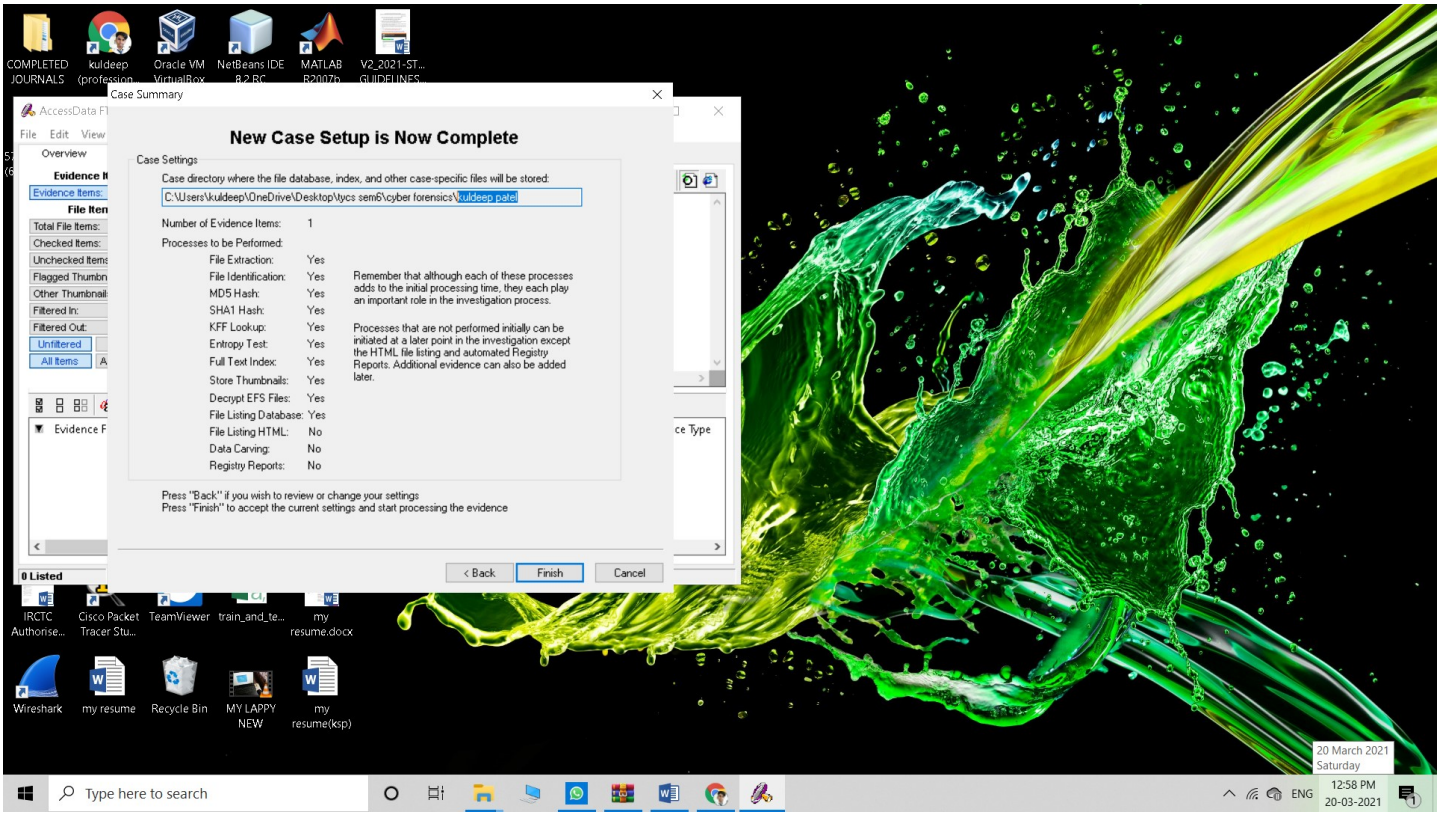
- Email protocols

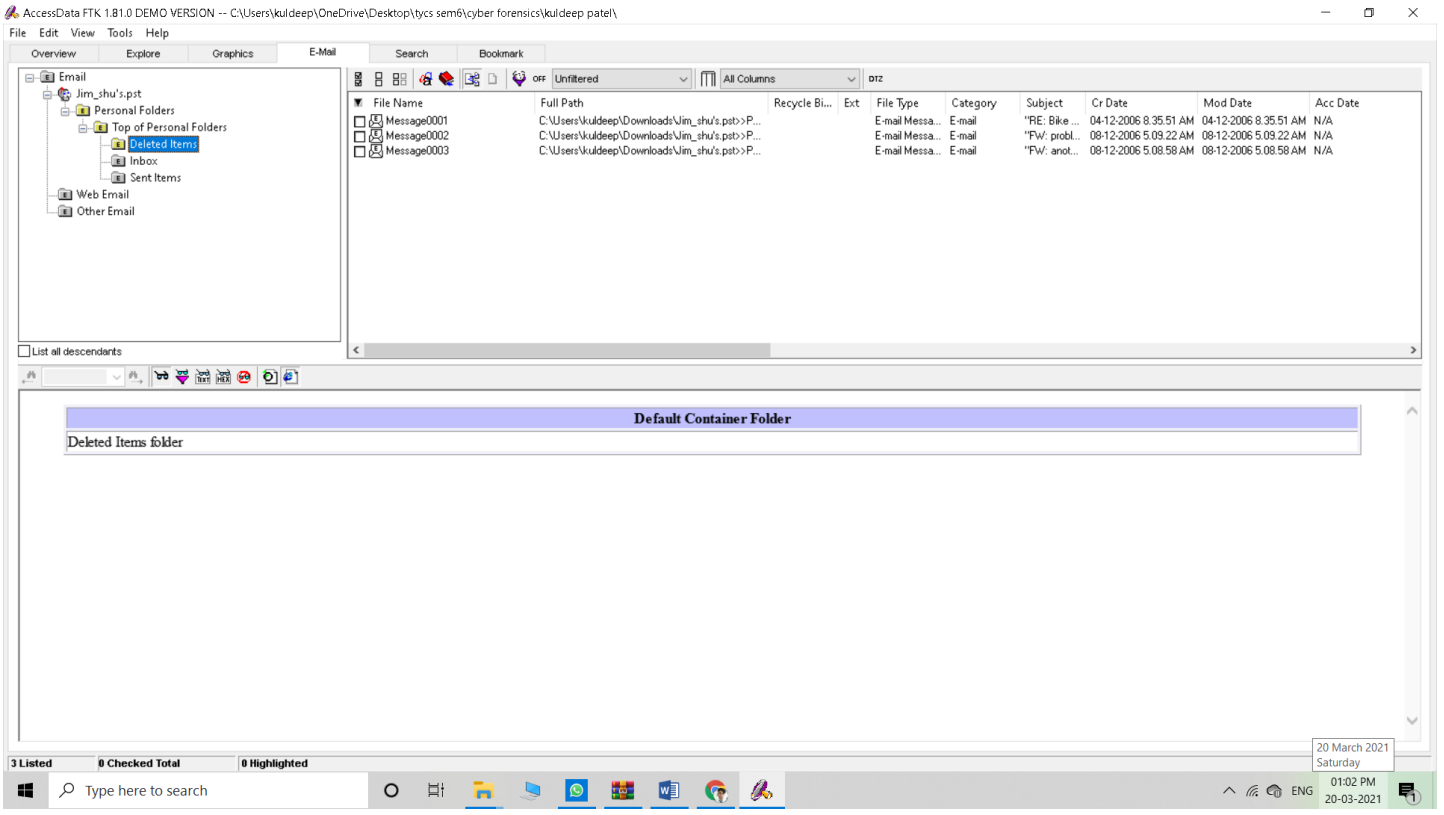
- Recovering emails

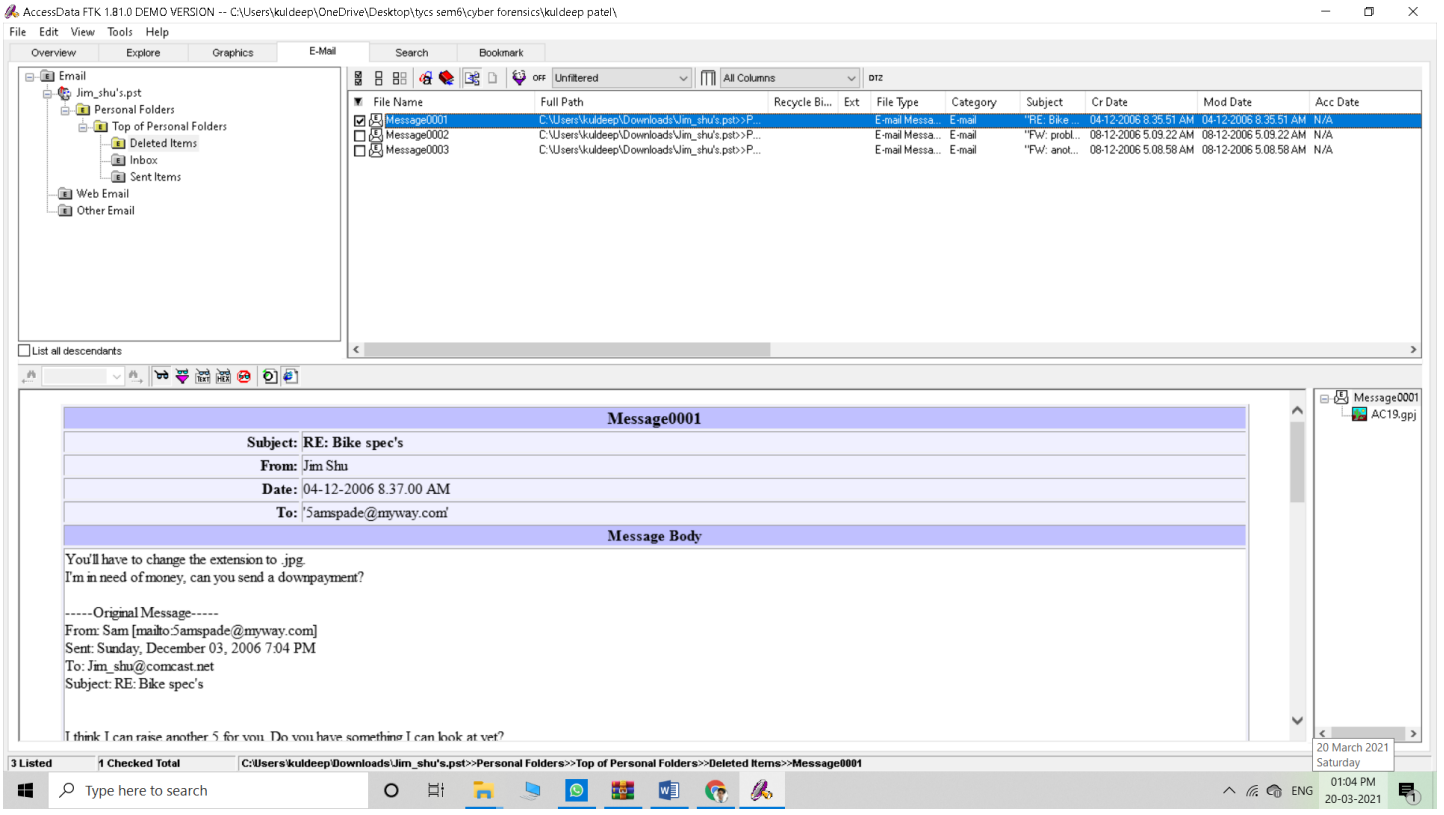
- Analysing email header

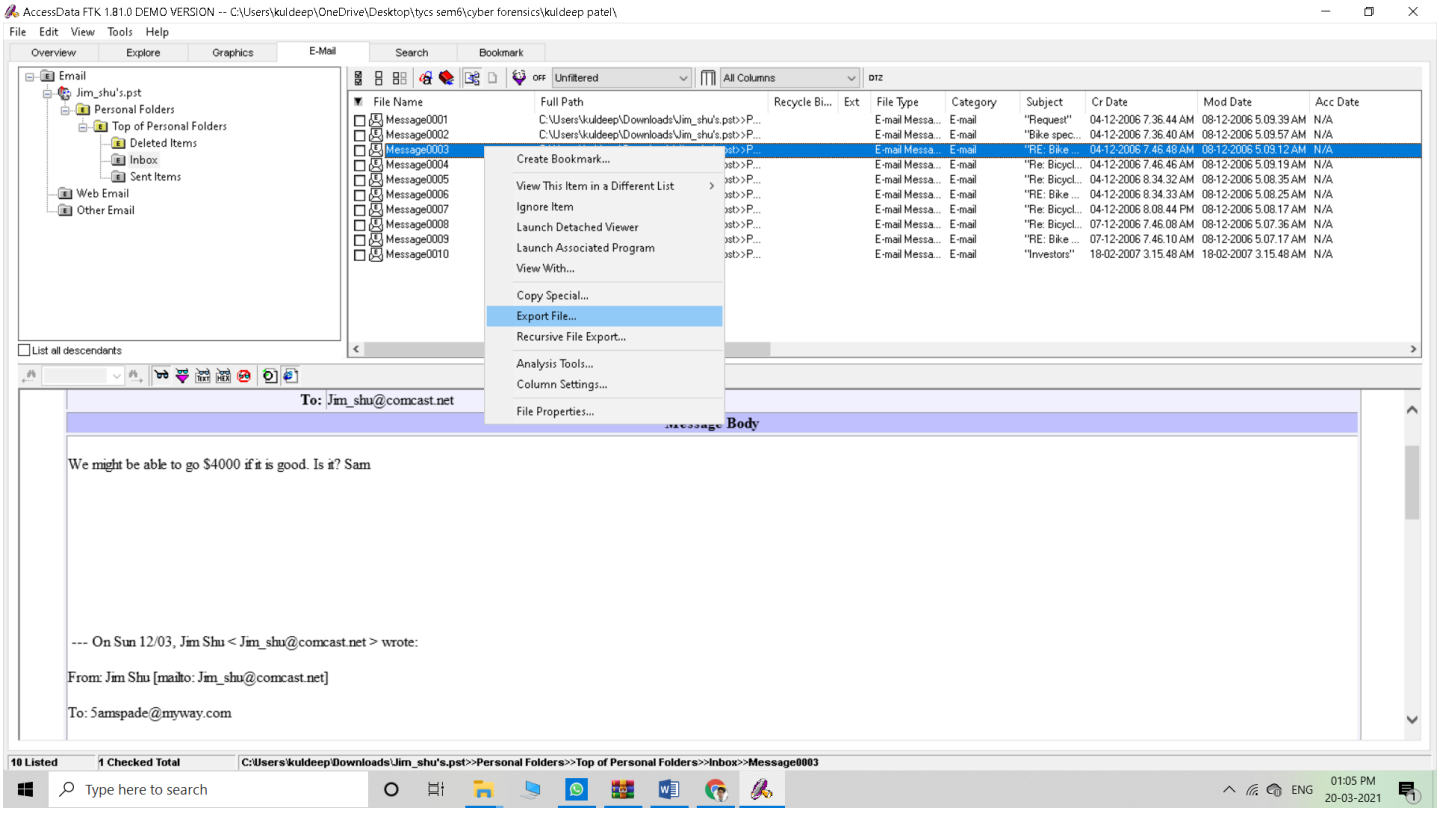
- FTK can filter or find files specific to e-mail clients and servers. You can configure these filters when you enter search parameters.
- Because of Jim's responses to a poor performance review, the CEO of Superior Bicycles,
- Martha Dax, suspects he might have obtained sensitive information about the company's business model that he's leaking to a competitor.
- Martha asked her CIO, to have an IT employee copy the Outlook .pst file from Jim Shu's old computer to a USB drive. To process this investigation,
- we need to examine the Jim_shu's.pst file, locate the message, and export it for further analysis of its header to see how Jim might have received it.
- Recovering Email Start AccessData FTK and click Start a new case, then click OK.
- Click Next until you reach the Refine Case - Default dialog box Click the Email Emphasis button , and then click Next .

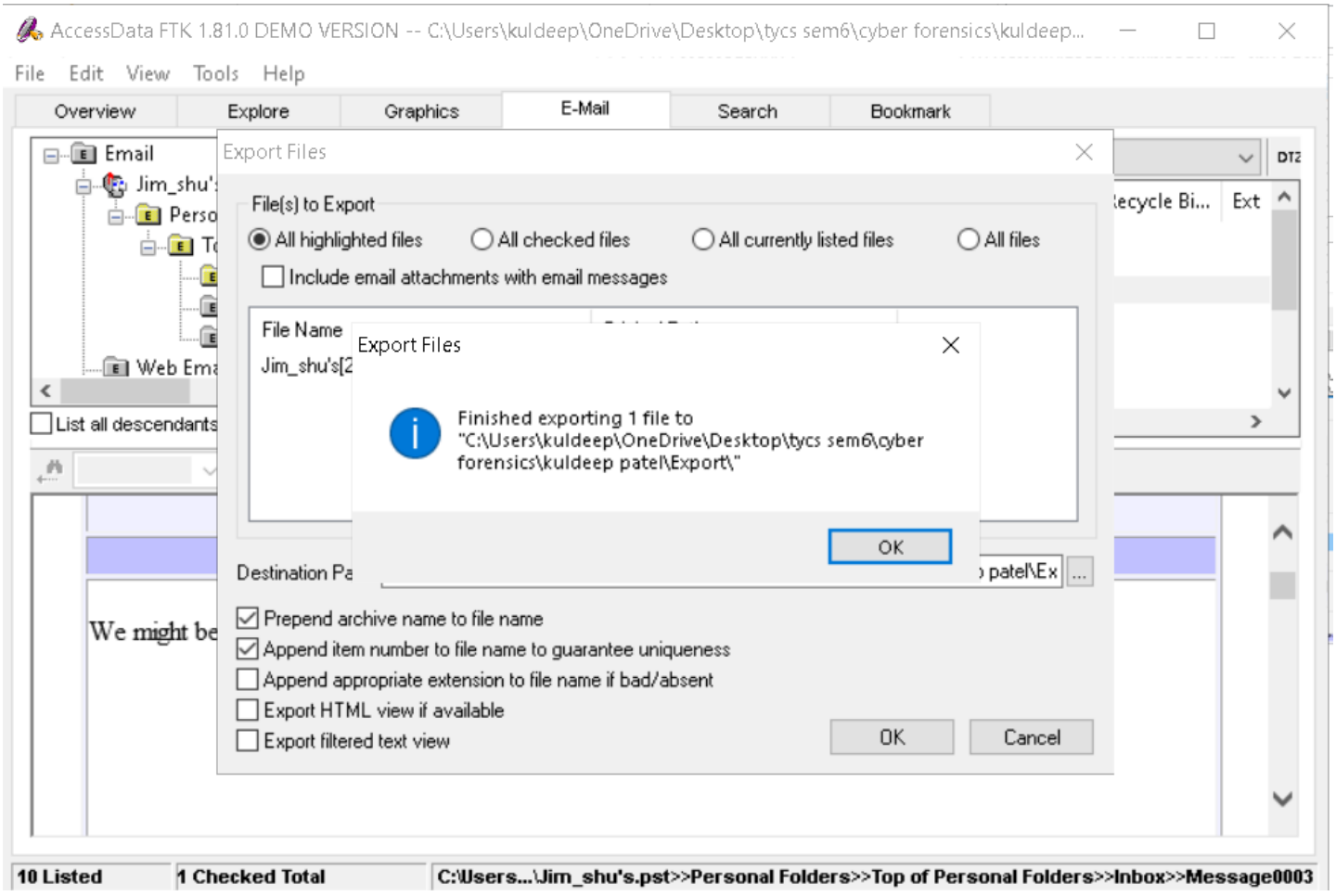

AccessData FTK 1.81.0 DEMO VERSION
File Edit View Tools Help
Overview Explore Graphics E-Mail
Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...
Add Evidence... Edit Evidence... Remove Evidence Refine Evidence - Advanced...
Display Name Source Name/Nu... Type Refined Time Zone Comment
Jim_shu's C:\Users\kuld... Individual f... N N/A
< Back Next > Cancel
0 Listed
Type here to search
20 March 2021 Saturday
ENG 12:57 PM 20-03-2021


Case Summary
New Case Setup is Now Complete
Case Settings
Case directory where the file database, index, and other case-specific files will be stored:
C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics\kuldeep patel
Number of Evidence Items: 1
Processes to be Performed:
File Extraction: Yes
File Identification: Yes
MD5 Hash: Yes
SHA1 Hash: Yes
KFF Lookup: Yes
Entropy Test: Yes
Full Text Index: Yes
Store Thumbnails: Yes
Decrypt EFS Files: Yes
File Listing Database: Yes
File Listing HTML: No
Data Carving: No
Registry Reports: No
Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.
Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence
< Back Finish Cancel
0 Listed
Type here to search
20 March 2021 Saturday
ENG 12:58 PM 20-03-2021

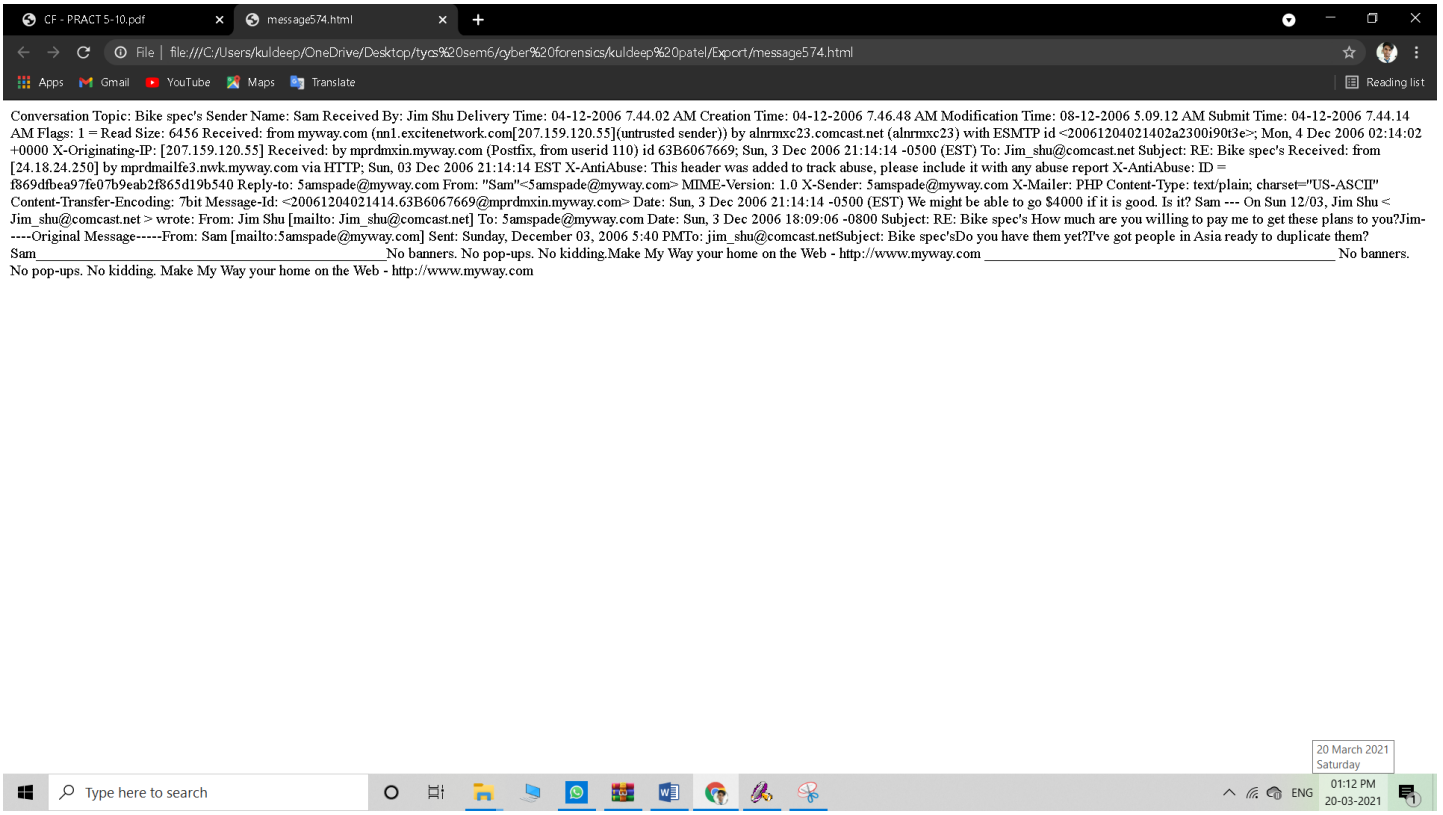

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics\kuldeep patel\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Email
Jim_shu's.pst
Personal Folders
Top of Personal Folders
Deleted Items
Inbox
Sent Items
Web Email
Other Email
List all descendants
Unfiltered
All Columns
File Name Full Path Recycle Bi... Ext File Type Category Subject Cr Date Mod Date Acc Date
Message0001 C:\Users\kuldeep\Downloads\Jim_shu's.pst>>P... E-mail Messa... E-mail "RE: Bike ... 04-12-2006 8.35.51 AM 04-12-2006 8.35.51 AM N/A
Message0002 C:\Users\kuldeep\Downloads\Jim_shu's.pst>>P... E-mail Messa... E-mail "FW: probl... 08-12-2006 5.09.22 AM 08-12-2006 5.09.22 AM N/A
Message0003 C:\Users\kuldeep\Downloads\Jim_shu's.pst>>P... E-mail Messa... E-mail "FW: anot... 08-12-2006 5.08.58 AM 08-12-2006 5.08.58 AM N/A
Default Container Folder
Deleted Items folder
3 Listed 0 Checked Total 0 Highlighted
20 March 2021 Saturday
Type here to search
ENG 01:02 PM 20-03-2021


AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics\kuldeep patel\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Email
Jim_shu's.pst
Personal Folders
Top of Personal Folders
Deleted Items
Inbox
Sent Items
Web Email
Other Email
List all descendants
Unfiltered
All Columns
File Name Full Path Recycle Bi... Ext File Type Category Subject Cr Date Mod Date Acc Date
Message0001 C:\Users\kuldeep\Downloads\Jim_shu's.pst>>P... E-mail Messa... E-mail "RE: Bike ... 04-12-2006 8.35.51 AM 04-12-2006 8.35.51 AM N/A
Message0002 C:\Users\kuldeep\Downloads\Jim_shu's.pst>>P... E-mail Messa... E-mail "FW: probl... 08-12-2006 5.09.22 AM 08-12-2006 5.09.22 AM N/A
Message0003 C:\Users\kuldeep\Downloads\Jim_shu's.pst>>P... E-mail Messa... E-mail "FW: anot... 08-12-2006 5.08.58 AM 08-12-2006 5.08.58 AM N/A
Message0001
Subject: RE: Bike spec's
From: Jim Shu
Date: 04-12-2006 8.37.00 AM
To: '5amspade@myway.com'
Message Body
You'll have to change the extension to .jpg.
I'm in need of money, can you send a downpayment?
-----Original Message-----
From: Sam [mailto:5amspade@myway.com]
Sent: Sunday, December 03, 2006 7:04 PM
To: Jim_shu@comcast.net
Subject: RE: Bike spec's
I think I can raise another 5 for you. Do you have something I can look at yet?
Message0001
AC19.gpj
3 Listed 1 Checked Total C:\Users\kuldeep\Downloads\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Deleted Items>>Message0001
20 March 2021 Saturday
Type here to search
ENG 01:04 PM 20-03-2021


AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics\kuldeep patel\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Email
Jim_shu's.pst
Personal Folders
Top of Personal Folders
Deleted Items
Inbox
Sent Items
Web Email
Other Email
List all descendants
Unfiltered
All Columns
File Name Full Path Recycle Bi... Ext File Type Category Subject Cr Date Mod Date Acc Date
Message0001 C:\Users\kuldeep\Downloads\Jim_shu's.pst>>P... E-mail Messa... E-mail "Request" 04-12-2006 7:36:44 AM 08-12-2006 5:09:39 AM N/A
Message0002 C:\Users\kuldeep\Downloads\Jim_shu's.pst>>P... E-mail Messa... E-mail "Bike spec... 04-12-2006 7:36:40 AM 08-12-2006 5:09:57 AM N/A
Message0003 E-mail Messa... E-mail "RE: Bike ... 04-12-2006 7:46:48 AM 08-12-2006 5:09:12 AM N/A
Message0004 E-mail Messa... E-mail "Re: Bicycl... 04-12-2006 7:46:46 AM 08-12-2006 5:09:19 AM N/A
Message0005 E-mail Messa... E-mail "Re: Bicycl... 04-12-2006 8:34:32 AM 08-12-2006 5:08:35 AM N/A
Message0006 E-mail Messa... E-mail "RE: Bike ... 04-12-2006 8:34:33 AM 08-12-2006 5:08:25 AM N/A
Message0007 E-mail Messa... E-mail "Re: Bicycl... 04-12-2006 8:08:44 PM 08-12-2006 5:08:17 AM N/A
Message0008 E-mail Messa... E-mail "Re: Bicycl... 07-12-2006 7:46:08 AM 08-12-2006 5:07:36 AM N/A
Message0009 E-mail Messa... E-mail "RE: Bike ... 07-12-2006 7:46:10 AM 08-12-2006 5:07:17 AM N/A
Message0010 E-mail Messa... E-mail "Investors" 18-02-2007 3:15:48 AM 18-02-2007 3:15:48 AM N/A
Create Bookmark...
View This Item in a Different List
Ignore Item
Launch Detached Viewer
Launch Associated Program
View With...
Copy Special...
Export File...
Recursive File Export...
Analysis Tools...
Column Settings...
File Properties...
To: Jim_shu@comcast.net
Message Body
We might be able to go $4000 if it is good. Is it? Sam
--- On Sun 12/03, Jim Shu < Jim_shu@comcast.net > wrote:
From: Jim Shu [mailto: Jim_shu@comcast.net]
To: 5amspade@myway.com
10 Listed 1 Checked Total C:\Users\kuldeep\Downloads\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Inbox>>Message0003
Type here to search
ENG
01:05 PM
20-03-2021


AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics\kuldeep...
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Email
Export Files
File(s) to Export
All highlighted files
All checked files
All currently listed files
All files
Include email attachments with email messages
File Name
Export Files
Finished exporting 1 file to "C:\Users\kuldeep\OneDrive\Desktop\tycs sem6\cyber forensics\kuldeep patel\Export\"
OK
Destination Pa
Prepend archive name to file name
Append item number to file name to guarantee uniqueness
Append appropriate extension to file name if bad/absent
Export HTML view if available
Export filtered text view
OK
Cancel
List all descendants
10 Listed
1 Checked Total
C:\Users...\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Inbox>>Message0003

Output :

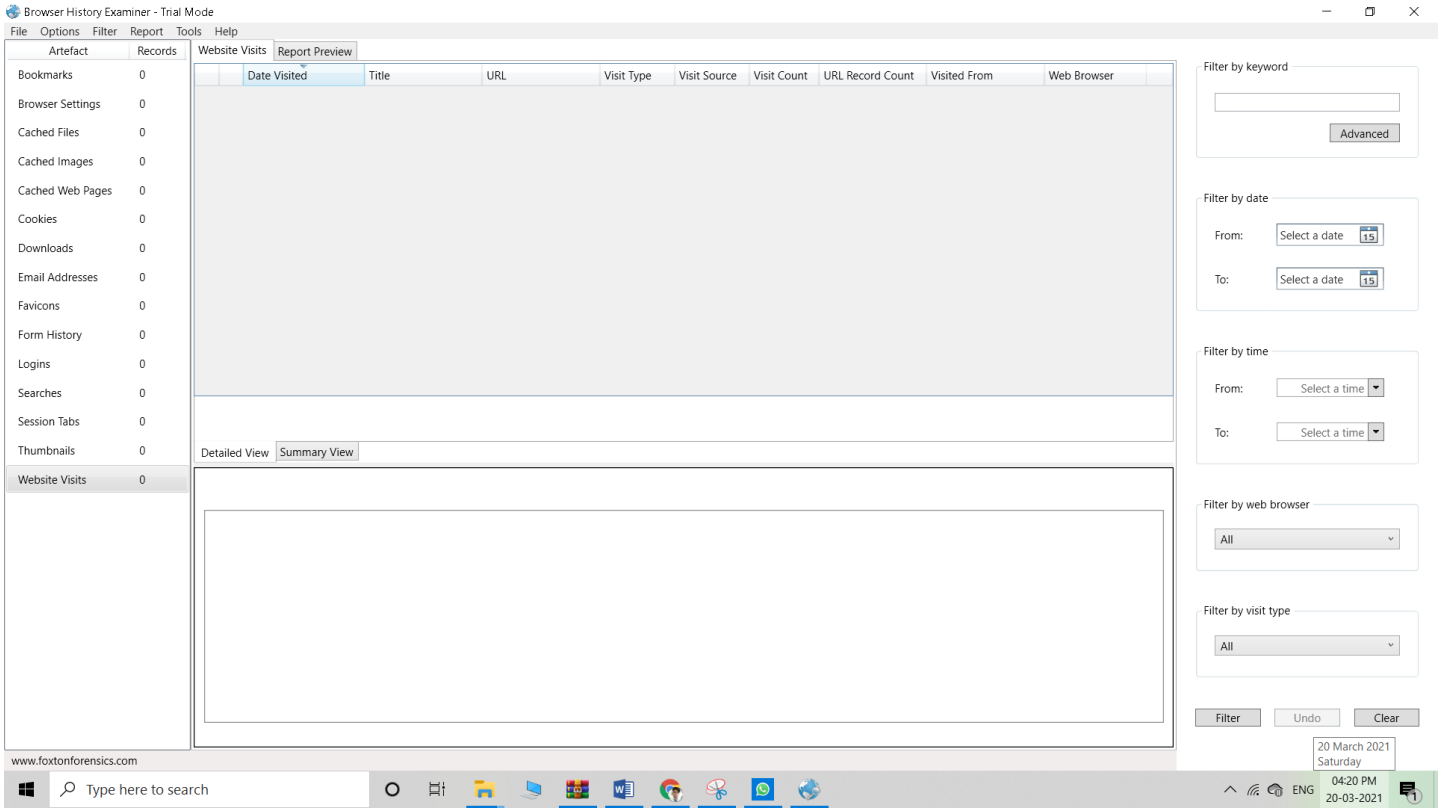

CF - PRACT 5-10.pdf
message574.html
file:///C:/Users/kuldeep/OneDrive/Desktop/tycs%20sem6/cyber%20forensics/kuldeep%20patel/Export/message574.html
Apps
Gmail
YouTube
Maps
Translate
Reading list
Conversation Topic: Bike spec's Sender Name: Sam Received By: Jim Shu Delivery Time: 04-12-2006 7.44.02 AM Creation Time: 04-12-2006 7.46.48 AM Modification Time: 08-12-2006 5.09.12 AM Submit Time: 04-12-2006 7.44.14 AM Flags: 1 = Read Size: 6456 Received: from myway.com (nn1.excitenetwork.com[207.159.120.55](untrusted sender)) by alnrmxc23.comcast.net (alnrmxc23) with ESMTP id <20061204021402a2300i90t3e>; Mon, 4 Dec 2006 02:14:02 +0000 X-Originating-IP: [207.159.120.55] Received: by mprdmxin.myway.com (Postfix, from userid 110) id 63B6067669; Sun, 3 Dec 2006 21:14:14 -0500 (EST) To: Jim_shu@comcast.net Subject: RE: Bike spec's Received: from [24.18.24.250] by mprdmailfe3.nwk.myway.com via HTTP; Sun, 03 Dec 2006 21:14:14 EST X-AntiAbuse: This header was added to track abuse, please include it with any abuse report X-AntiAbuse: ID = f869dfbea97fe07b9eab2f865d19b540 Reply-to: 5amspade@myway.com From: "Sam"<5amspade@myway.com> MIME-Version: 1.0 X-Sender: 5amspade@myway.com X-Mailer: PHP Content-Type: text/plain; charset="US-ASCII" Content-Transfer-Encoding: 7bit Message-Id: <20061204021414.63B6067669@mprdmxin.myway.com> Date: Sun, 3 Dec 2006 21:14:14 -0500 (EST) We might be able to go $4000 if it is good. Is it? Sam --- On Sun 12/03, Jim Shu < Jim_shu@comcast.net > wrote: From: Jim Shu [mailto: Jim_shu@comcast.net] To: 5amspade@myway.com Date: Sun, 3 Dec 2006 18:09:06 -0800 Subject: RE: Bike spec's How much are you willing to pay me to get these plans to you?Jim- ----Original Message-----From: Sam [mailto:5amspade@myway.com] Sent: Sunday, December 03, 2006 5:40 PMTo: jim_shu@comcast.netSubject: Bike spec'sDo you have them yet?I've got people in Asia ready to duplicate them? Sam_____No banners. No pop-ups. No kidding.Make My Way your home on the Web - http://www.myway.com _____ No banners. No pop-ups. No kidding. Make My Way your home on the Web - http://www.myway.com
Type here to search
20 March 2021
Saturday
ENG
01:12 PM
20-03-2021

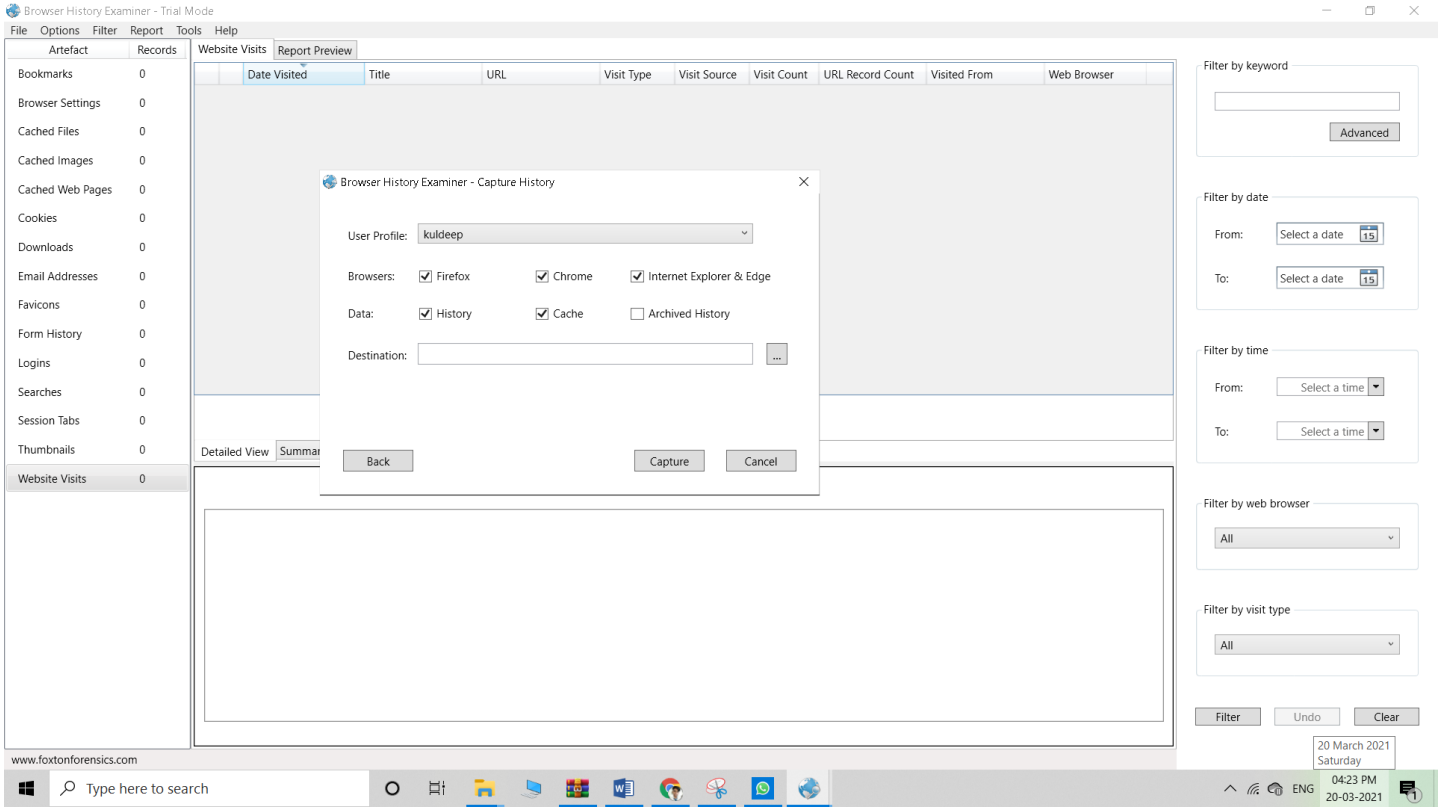
Practical no 10

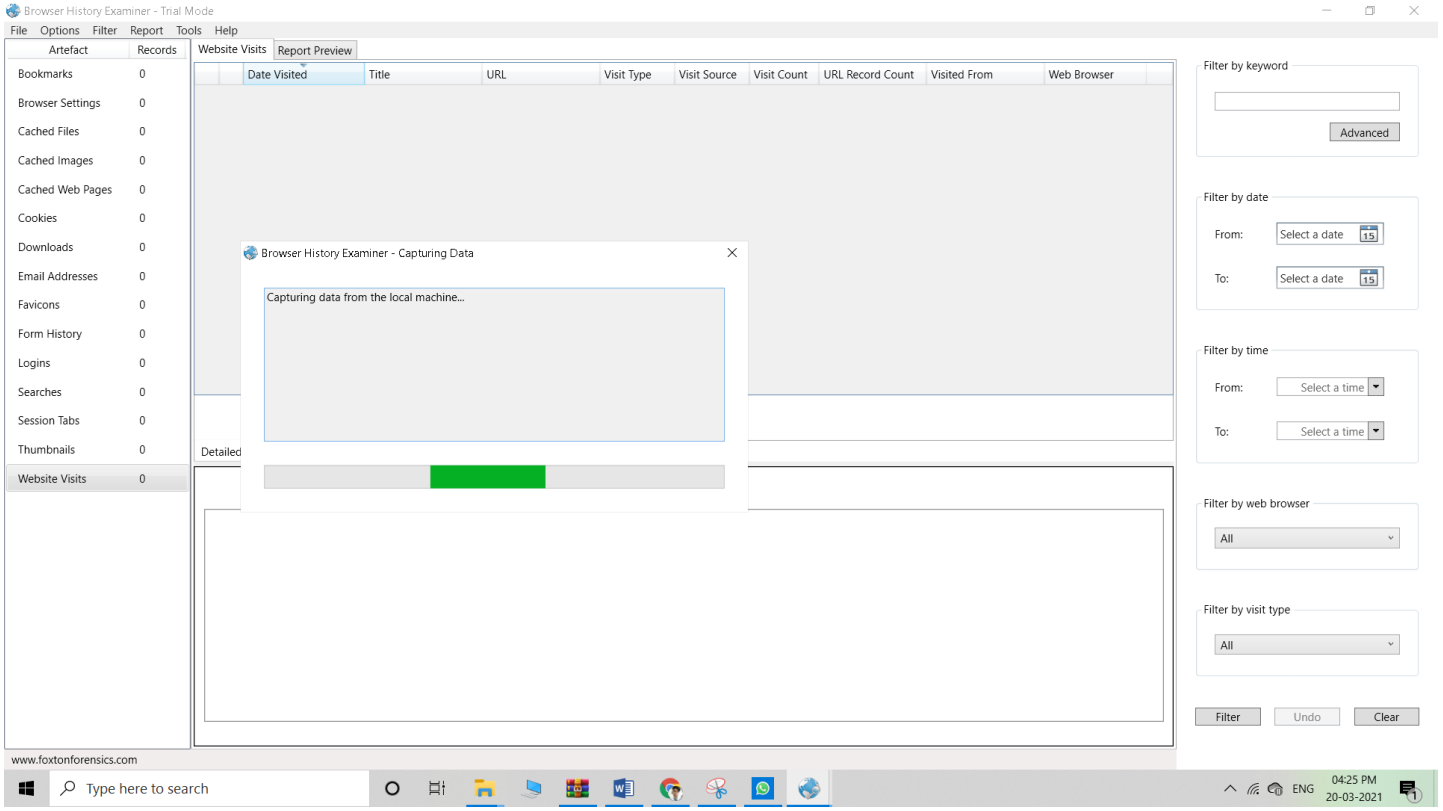
Aim: Web Browser Forensics.

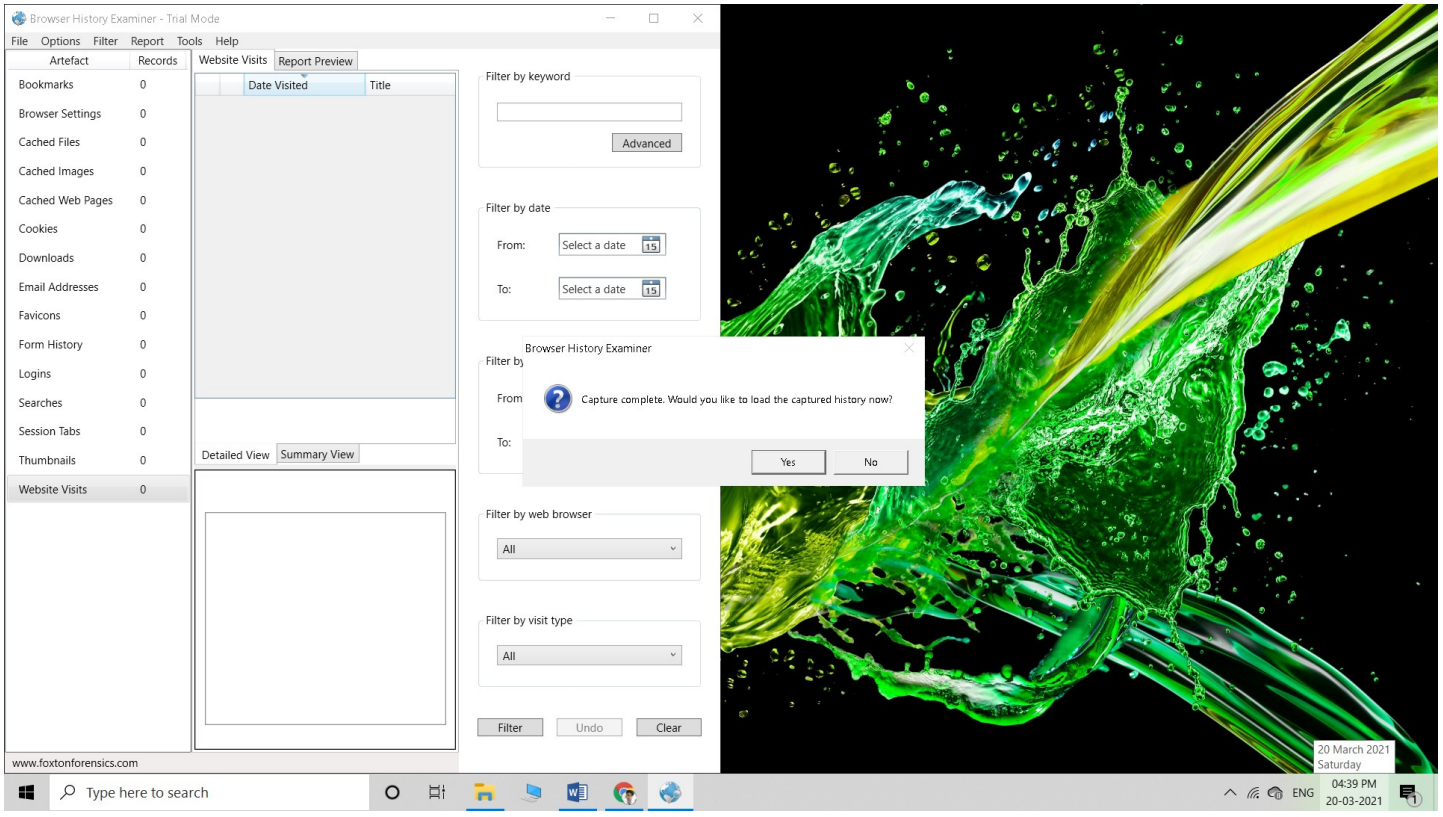
-Web Browser working
-Forensics activities on browser
-Cache / Cookies analysis
-Last Internet activity

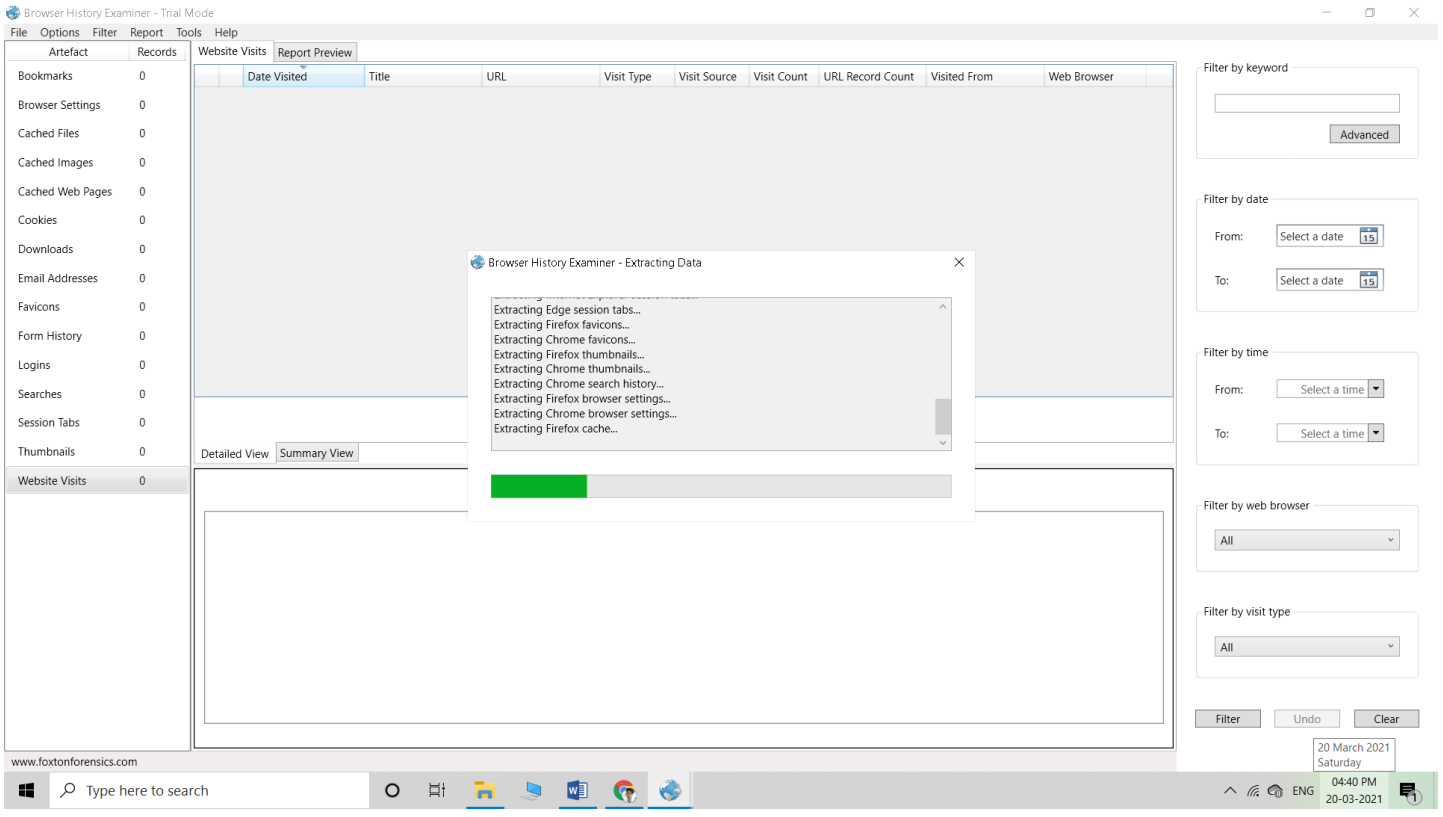
Steps: 1. Open BrowserHistoryExaminer.

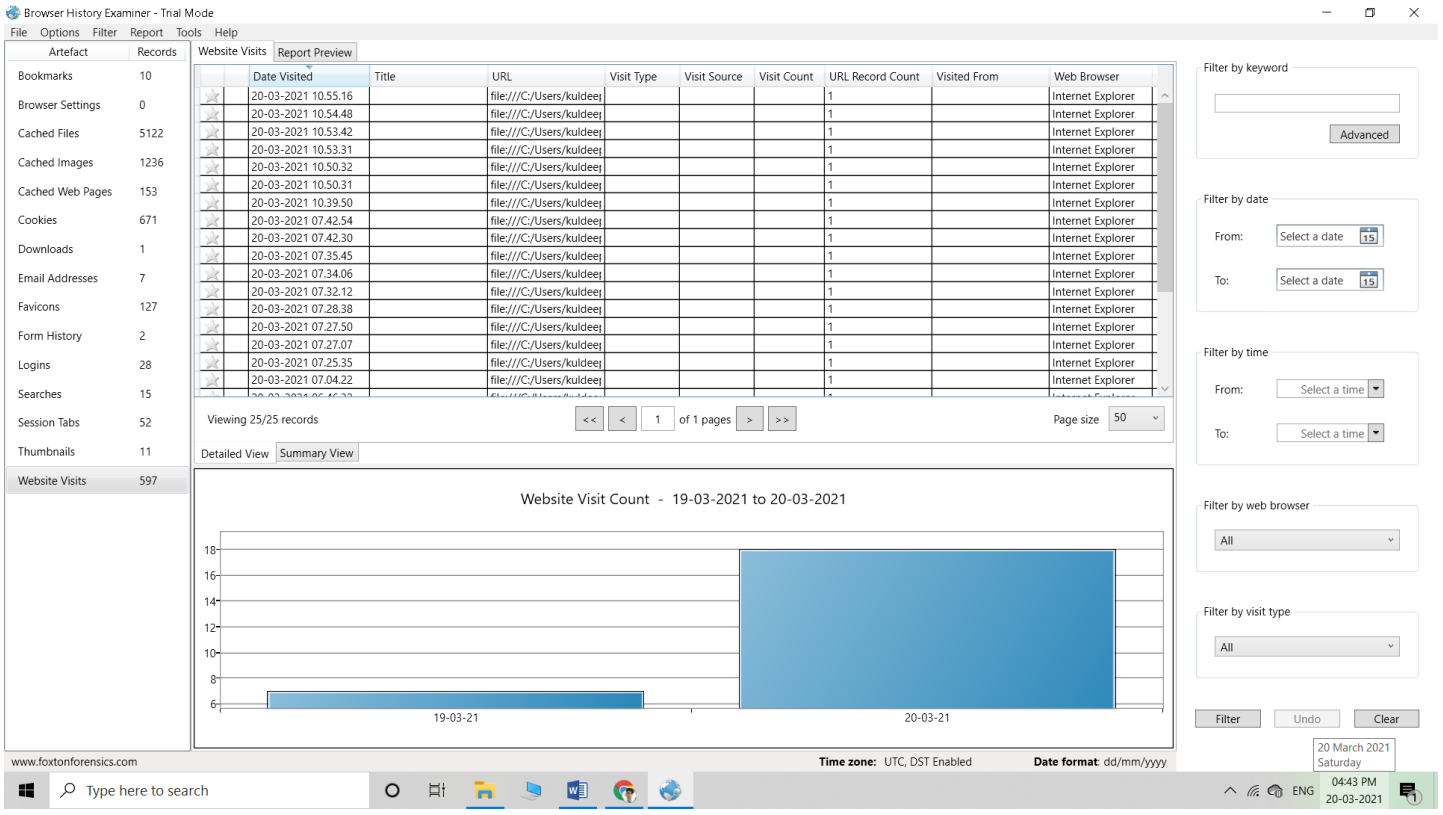


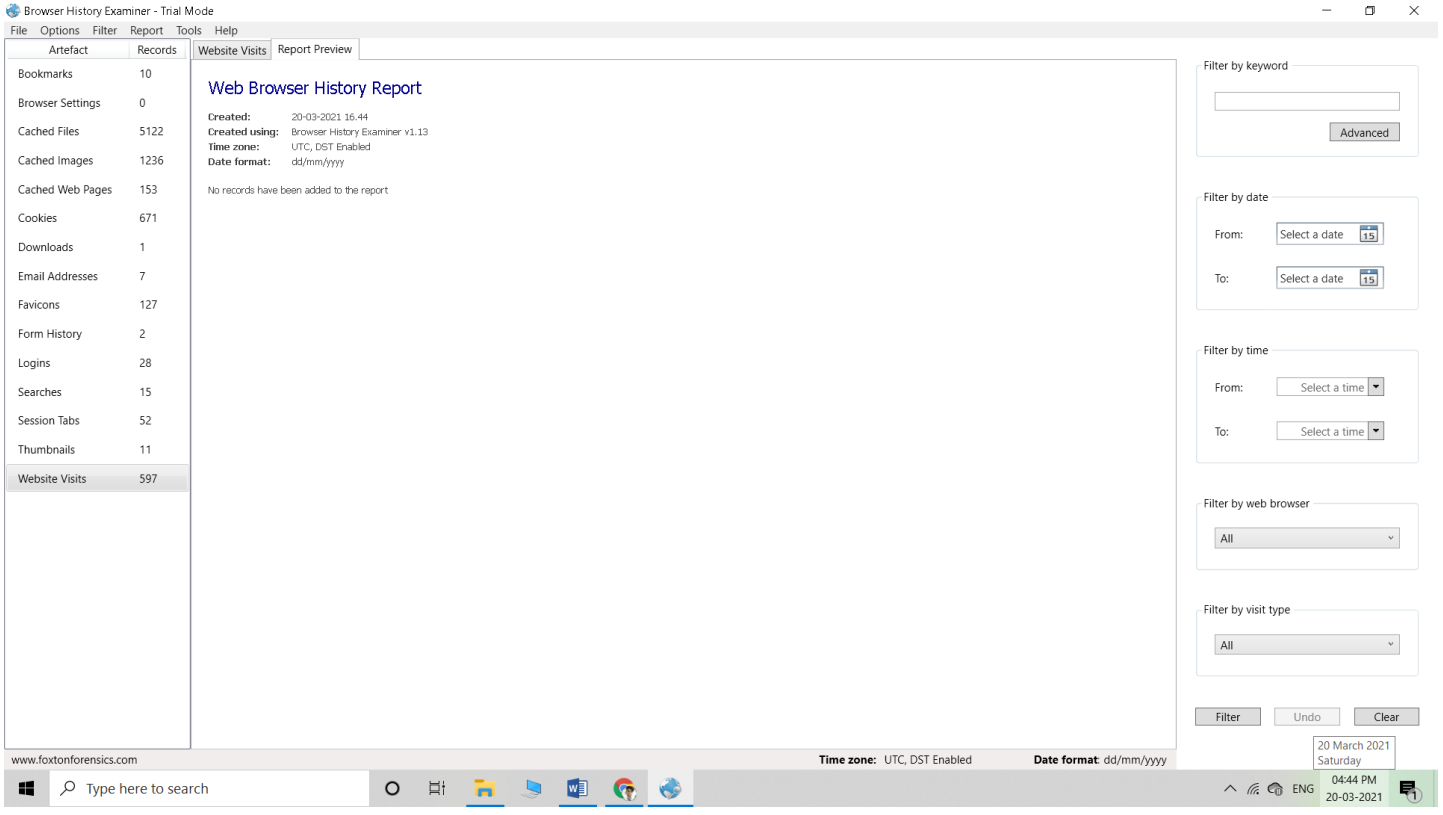

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 0
Browser Settings 0
Cached Files 0
Cached Images 0
Cached Web Pages 0
Cookies 0
Downloads 0
Email Addresses 0
Favicons 0
Form History 0
Logins 0
Searches 0
Session Tabs 0
Thumbnails 0
Website Visits 0
Website Visits
Report Preview
Date Visited
Title
URL
Visit Type
Visit Source
Visit Count
URL Record Count
Visited From
Web Browser
Browser History Examiner - Capture History
User Profile: kuldeep
Browsers: Firefox Chrome Internet Explorer & Edge
Data: History Cache Archived History
Destination:
Back
Capture
Cancel
Detailed View
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter by visit type
All
Filter
Undo
Clear
www.foxtonforensics.com
20 March 2021
Saturday
Type here to search
ENG
04:23 PM
20-03-2021

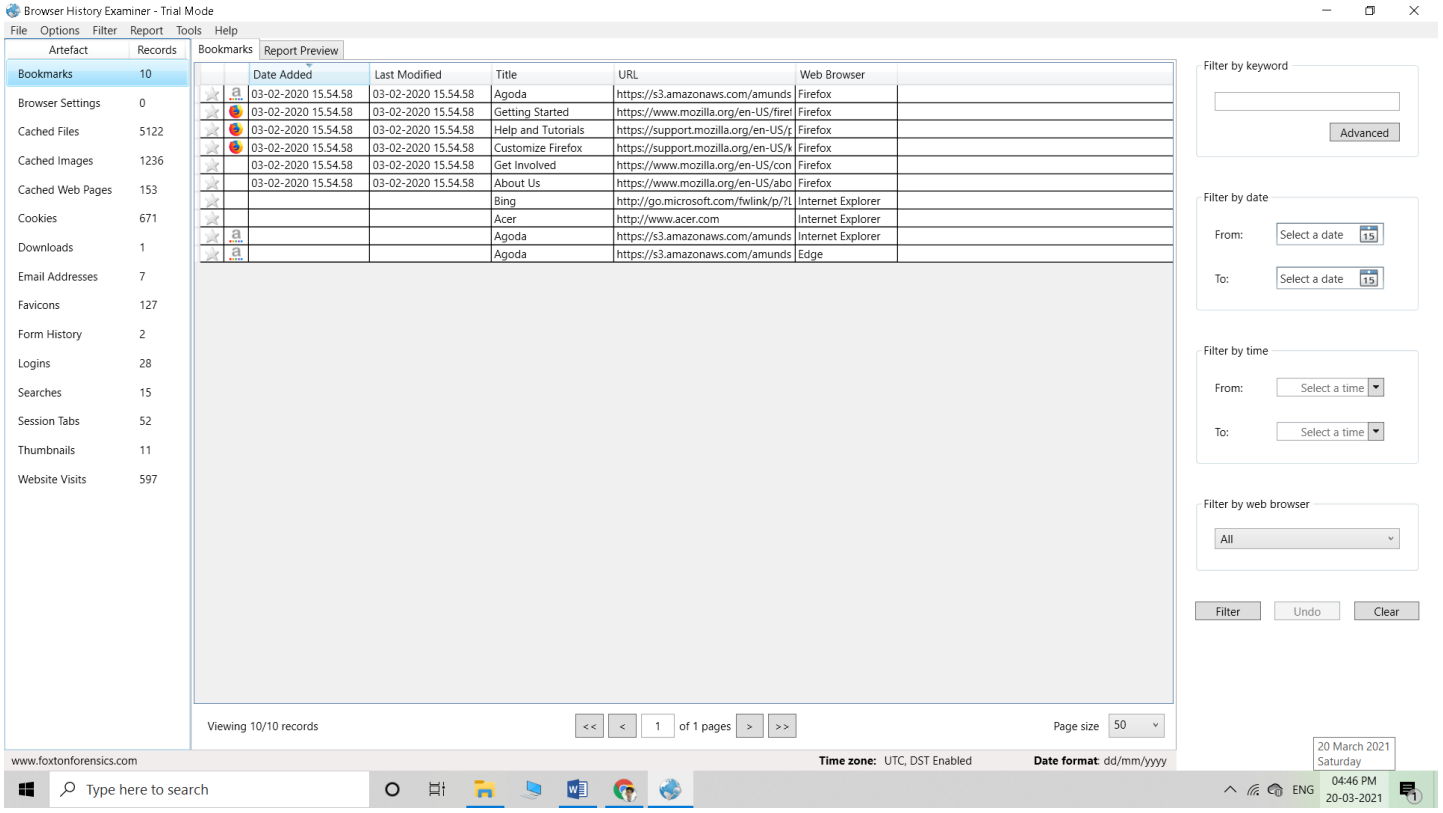

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 0
Browser Settings 0
Cached Files 0
Cached Images 0
Cached Web Pages 0
Cookies 0
Downloads 0
Email Addresses 0
Favicons 0
Form History 0
Logins 0
Searches 0
Session Tabs 0
Thumbnails 0
Website Visits 0
Website Visits
Report Preview
Date Visited
Title
URL
Visit Type
Visit Source
Visit Count
URL Record Count
Visited From
Web Browser
Browser History Examiner - Capturing Data
Capturing data from the local machine...
Detailed
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter by visit type
All
Filter
Undo
Clear
www.foxtonforensics.com
Type here to search
ENG
04:25 PM
20-03-2021

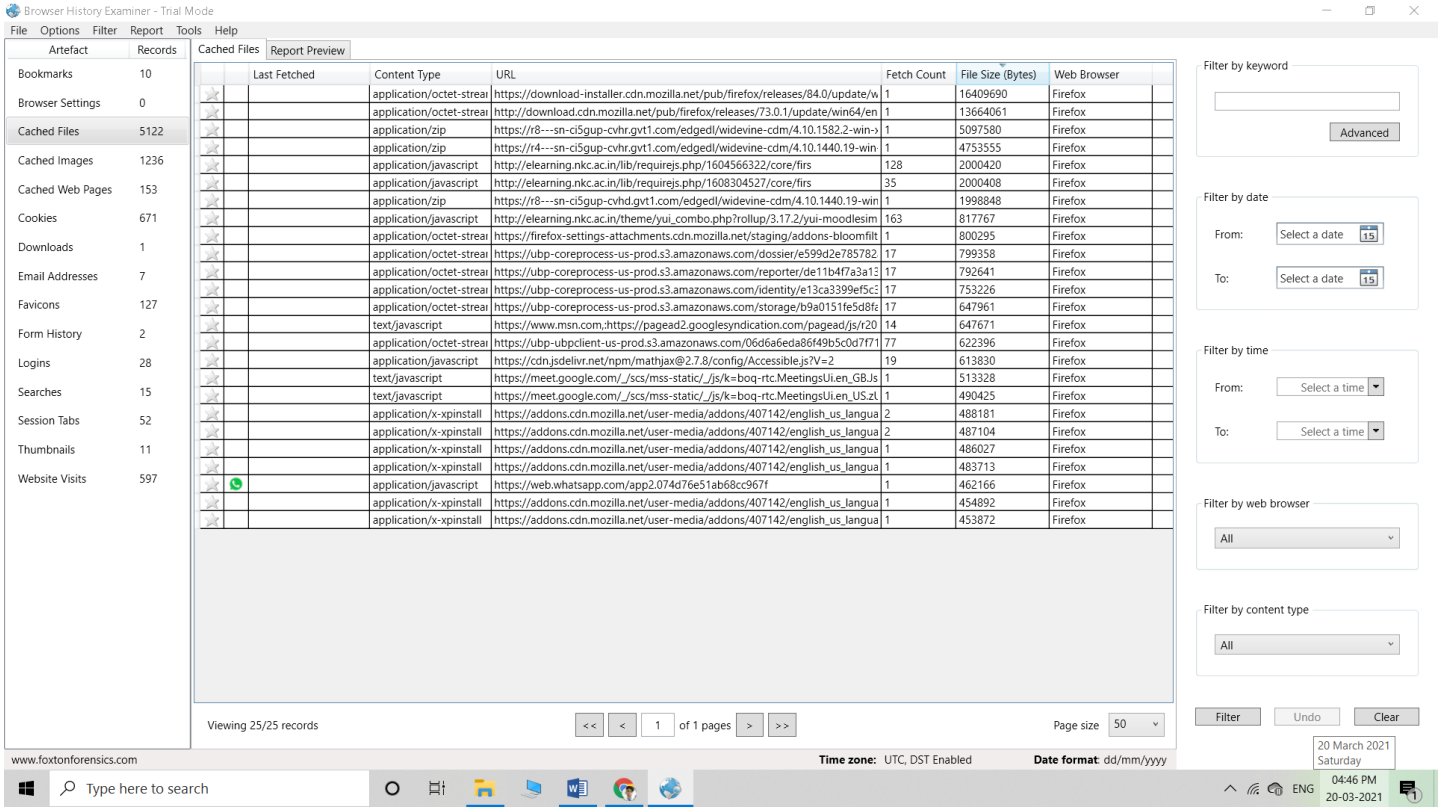

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 0
Browser Settings 0
Cached Files 0
Cached Images 0
Cached Web Pages 0
Cookies 0
Downloads 0
Email Addresses 0
Favicons 0
Form History 0
Logins 0
Searches 0
Session Tabs 0
Thumbnails 0
Website Visits 0
Website Visits
Report Preview
Date Visited
Title
Detailed View
Summary View
Filter by keyword
Advanced
Filter by date
From:
Select a date
To:
Select a date
Browser History Examiner
Capture complete. Would you like to load the captured history now?
Yes
No
Filter by web browser
All
Filter by visit type
All
Filter
Undo
Clear
www.foxtonforensics.com
20 March 2021
Saturday
Type here to search
ENG
04:39 PM
20-03-2021

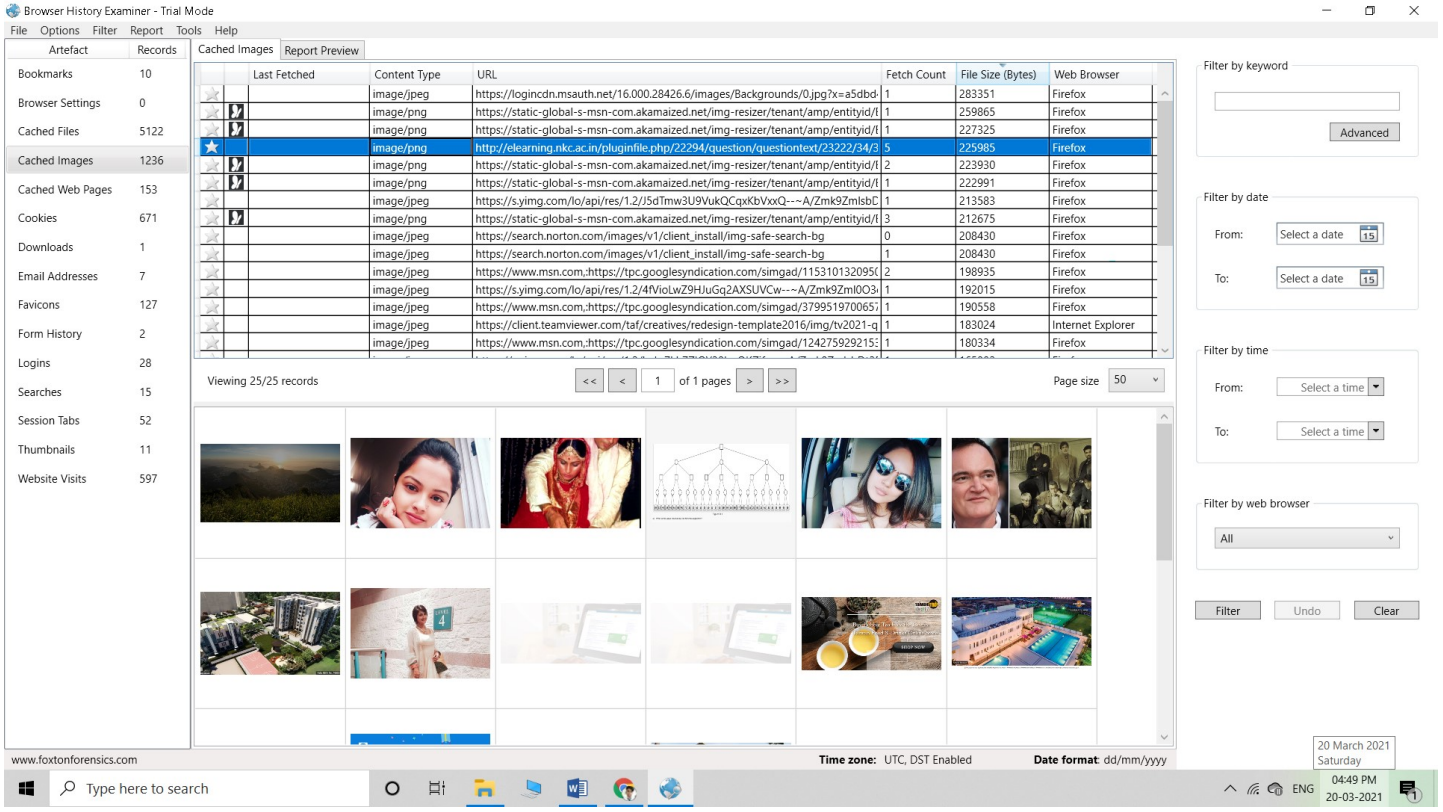

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 0
Browser Settings 0
Cached Files 0
Cached Images 0
Cached Web Pages 0
Cookies 0
Downloads 0
Email Addresses 0
Favicons 0
Form History 0
Logins 0
Searches 0
Session Tabs 0
Thumbnails 0
Website Visits 0
Website Visits
Report Preview
Date Visited
Title
URL
Visit Type
Visit Source
Visit Count
URL Record Count
Visited From
Web Browser
Browser History Examiner - Extracting Data
Extracting Edge session tabs...
Extracting Firefox favicons...
Extracting Chrome favicons...
Extracting Firefox thumbnails...
Extracting Chrome thumbnails...
Extracting Chrome search history...
Extracting Firefox browser settings...
Extracting Chrome browser settings...
Extracting Firefox cache...
Detailed View
Summary View
Filter by keyword
Advanced
Filter by date
From:
Select a date
To:
Select a date
Filter by time
From:
Select a time
To:
Select a time
Filter by web browser
All
Filter by visit type
All
Filter
Undo
Clear
www.foxtonforensics.com
20 March 2021
Saturday
Type here to search
ENG
04:40 PM
20-03-2021

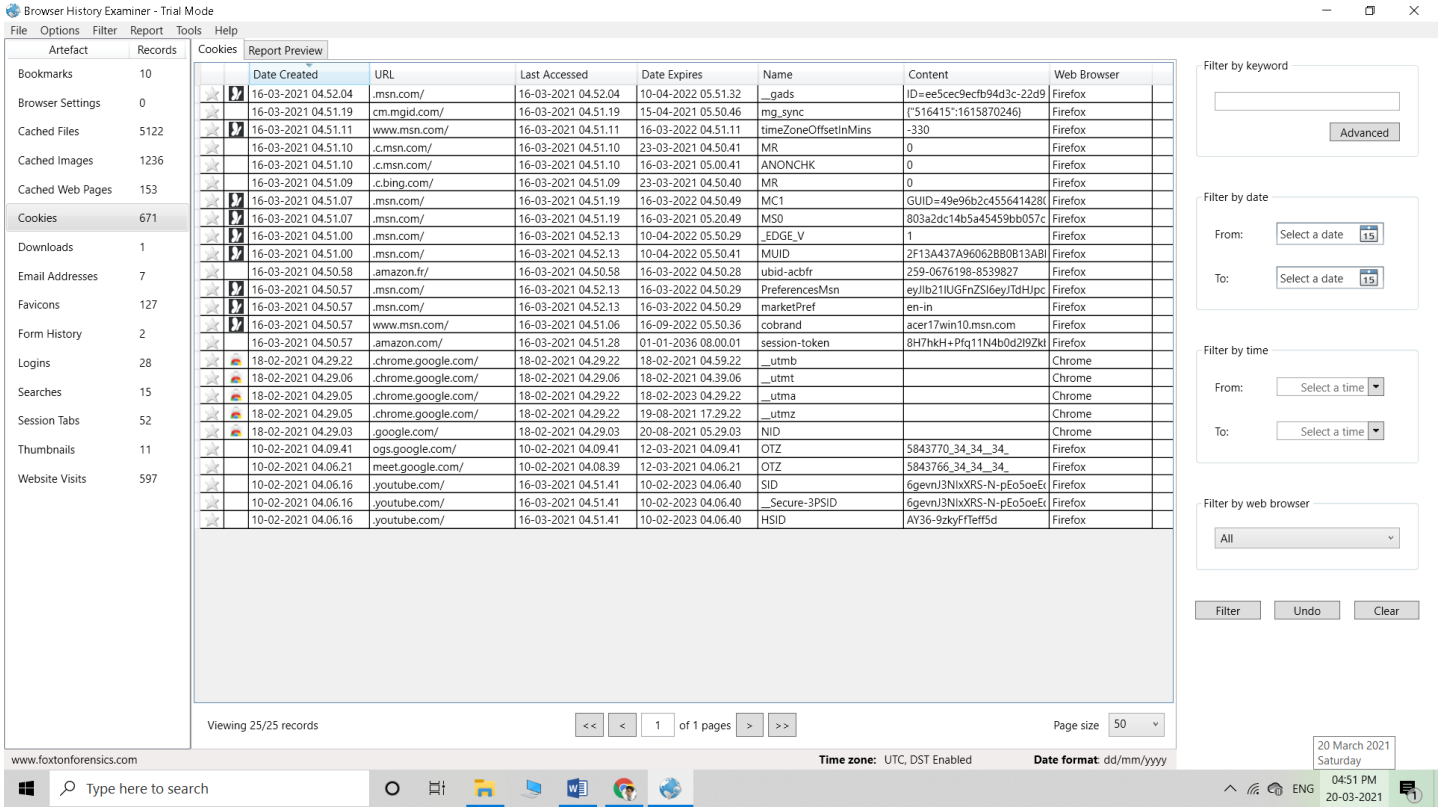

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 10
Browser Settings 0
Cached Files 5122
Cached Images 1236
Cached Web Pages 153
Cookies 671
Downloads 1
Email Addresses 7
Favicons 127
Form History 2
Logins 28
Searches 15
Session Tabs 52
Thumbnails 11
Website Visits 597
Website Visits
Report Preview
Date Visited
Title
URL
Visit Type
Visit Source
Visit Count
URL Record Count
Visited From
Web Browser
20-03-2021 10.55.16 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 10.54.48 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 10.53.42 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 10.53.31 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 10.50.32 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 10.50.31 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 10.39.50 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.42.54 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.42.30 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.35.45 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.34.06 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.32.12 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.28.38 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.27.50 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.27.07 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.25.35 file:///C:/Users/kuldeep Internet Explorer
20-03-2021 07.04.22 file:///C:/Users/kuldeep Internet Explorer
Viewing 25/25 records
<< < 1 of 1 pages > >>
Page size 50
Detailed View
Summary View
Website Visit Count - 19-03-2021 to 20-03-2021
18
16
14
12
10
8
6
19-03-21
20-03-21
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter by visit type
All
Filter
Undo
Clear
www.foxtonforensics.com
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy
20 March 2021
Saturday
Type here to search
ENG
04:43 PM
20-03-2021

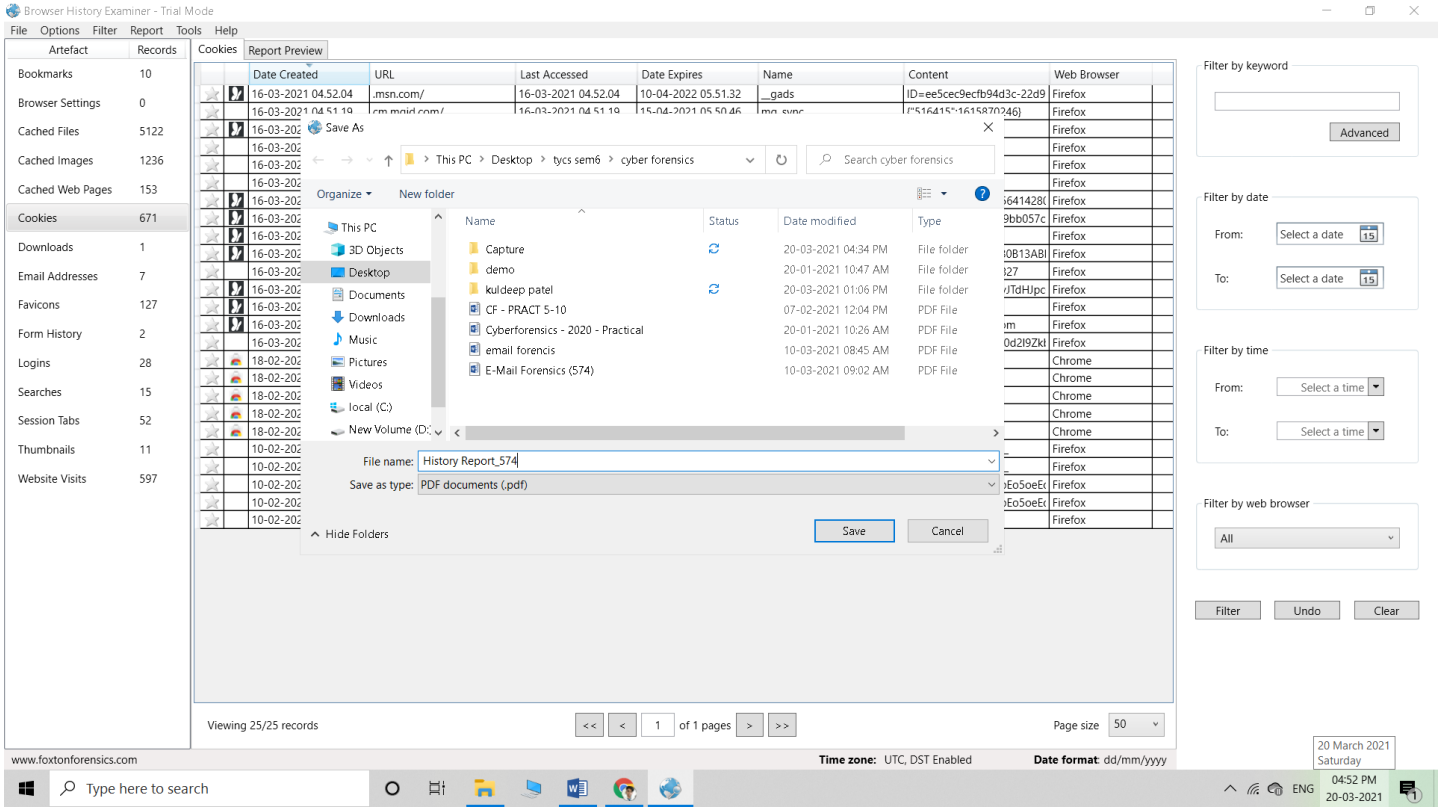

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 10
Browser Settings 0
Cached Files 5122
Cached Images 1236
Cached Web Pages 153
Cookies 671
Downloads 1
Email Addresses 7
Favicons 127
Form History 2
Logins 28
Searches 15
Session Tabs 52
Thumbnails 11
Website Visits 597
Website Visits
Report Preview
Web Browser History Report
Created: 20-03-2021 16.44
Created using: Browser History Examiner v1.13
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy
No records have been added to the report
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter by visit type
All
Filter
Undo
Clear
www.foxtonforensics.com
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy
20 March 2021
Saturday
Type here to search
ENG
04:44 PM
20-03-2021

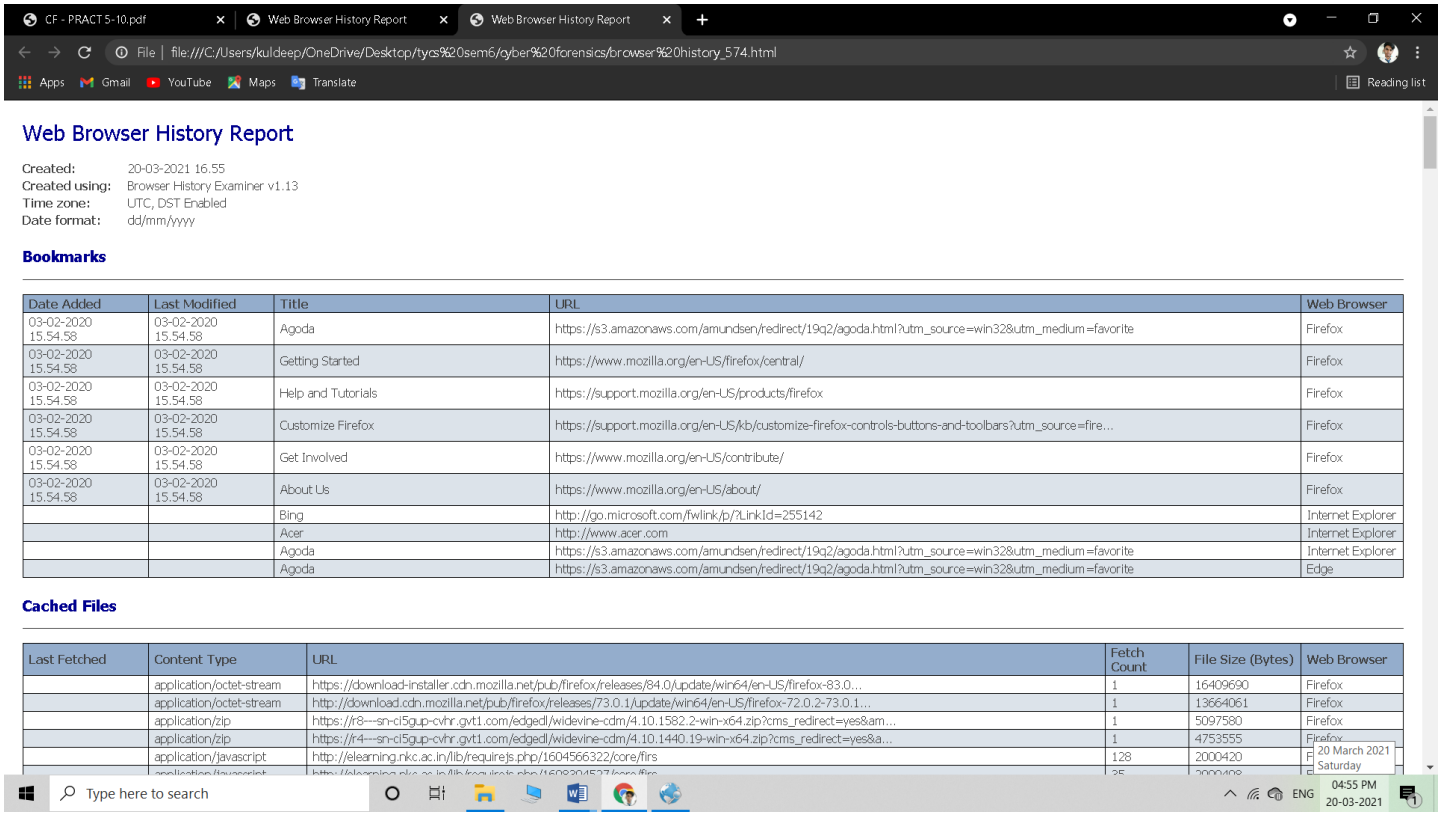

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 10
Browser Settings 0
Cached Files 5122
Cached Images 1236
Cached Web Pages 153
Cookies 671
Downloads 1
Email Addresses 7
Favicons 127
Form History 2
Logins 28
Searches 15
Session Tabs 52
Thumbnails 11
Website Visits 597
Bookmarks
Report Preview
Date Added
Last Modified
Title
URL
Web Browser
03-02-2020 15.54.58 03-02-2020 15.54.58 Agoda https://s3.amazonaws.com/amunds Firefox
03-02-2020 15.54.58 03-02-2020 15.54.58 Getting Started https://www.mozilla.org/en-US/firef Firefox
03-02-2020 15.54.58 03-02-2020 15.54.58 Help and Tutorials https://support.mozilla.org/en-US/p Firefox
03-02-2020 15.54.58 03-02-2020 15.54.58 Customize Firefox https://support.mozilla.org/en-US/k Firefox
03-02-2020 15.54.58 03-02-2020 15.54.58 Get Involved https://www.mozilla.org/en-US/con Firefox
03-02-2020 15.54.58 03-02-2020 15.54.58 About Us https://www.mozilla.org/en-US/abo Firefox
Bing http://go.microsoft.com/fwlink/p/?L Internet Explorer
Acer http://www.acer.com Internet Explorer
Agoda https://s3.amazonaws.com/amunds Internet Explorer
Agoda https://s3.amazonaws.com/amunds Edge
Viewing 10/10 records
<< < 1 of 1 pages > >>
Page size 50
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter Undo Clear
www.foxtonforensics.com
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy
20 March 2021 Saturday
Type here to search
ENG
04:46 PM 20-03-2021


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 10
Browser Settings 0
Cached Files 5122
Cached Images 1236
Cached Web Pages 153
Cookies 671
Downloads 1
Email Addresses 7
Favicons 127
Form History 2
Logins 28
Searches 15
Session Tabs 52
Thumbnails 11
Website Visits 597
Cached Files
Report Preview
Last Fetched
Content Type
URL
Fetch Count
File Size (Bytes)
Web Browser
application/octet-strea https://download-installer.cdn.mozilla.net/pub/firefox/releases/84.0/update/w 1 16409690 Firefox
application/octet-strea http://download.cdn.mozilla.net/pub/firefox/releases/73.0.1/update/win64/en 1 13664061 Firefox
application/zip https://r8---sn-ci5gup-cvhr.gvt1.com/edgedl/widevine-cdm/4.10.1582.2-win-x 1 5097580 Firefox
application/zip https://r4---sn-ci5gup-cvhr.gvt1.com/edgedl/widevine-cdm/4.10.1440.19-win 1 4753555 Firefox
application/javascript http://elearning.nkc.ac.in/lib/requirejs.php/1604566322/core/firs 128 2000420 Firefox
application/javascript http://elearning.nkc.ac.in/lib/requirejs.php/1608304527/core/firs 35 2000408 Firefox
application/zip https://r8---sn-ci5gup-cvhd.gvt1.com/edgedl/widevine-cdm/4.10.1440.19-win 1 1998848 Firefox
application/javascript http://elearning.nkc.ac.in/theme/yui_combo.php?rollup/3.17.2/yui-moodlesim 163 817767 Firefox
application/octet-strea https://firefox-settings-attachments.cdn.mozilla.net/staging/addons-bloomfilt 1 800295 Firefox
application/octet-strea https://ubp-coreprocess-us-prod.s3.amazonaws.com/dossier/e599d2e785782 17 799358 Firefox
application/octet-strea https://ubp-coreprocess-us-prod.s3.amazonaws.com/reporter/de11b4f7a3a13 17 792641 Firefox
application/octet-strea https://ubp-coreprocess-us-prod.s3.amazonaws.com/identity/e13ca3399ef5c3 17 753226 Firefox
application/octet-strea https://ubp-coreprocess-us-prod.s3.amazonaws.com/storage/b9a0151fe5d8fa 17 647961 Firefox
text/javascript https://www.msn.com,https://pagead2.googlesyndication.com/pagead/js/r20 14 647671 Firefox
application/octet-strea https://ubp-ubpclient-us-prod.s3.amazonaws.com/06d6a6eda86f49b5c0d7f71 77 622396 Firefox
application/javascript https://cdn.jsdelivr.net/npm/mathjax@2.7.8/config/Accessible.js?V=2 19 613830 Firefox
text/javascript https://meet.google.com/_/scs/mss-static/_/js/k=boq-rtc.MeetingsUi.en_GB.Js 1 513328 Firefox
text/javascript https://meet.google.com/_/scs/mss-static/_/js/k=boq-rtc.MeetingsUi.en_US.zL 1 490425 Firefox
application/x-xpinstall https://addons.cdn.mozilla.net/user-media/addons/407142/english_us_langua 2 488181 Firefox
application/x-xpinstall https://addons.cdn.mozilla.net/user-media/addons/407142/english_us_langua 2 487104 Firefox
application/x-xpinstall https://addons.cdn.mozilla.net/user-media/addons/407142/english_us_langua 1 486027 Firefox
application/x-xpinstall https://addons.cdn.mozilla.net/user-media/addons/407142/english_us_langua 1 483713 Firefox
application/javascript https://web.whatsapp.com/app2.074d76e51ab68cc967f 1 462166 Firefox
application/x-xpinstall https://addons.cdn.mozilla.net/user-media/addons/407142/english_us_langua 1 454892 Firefox
application/x-xpinstall https://addons.cdn.mozilla.net/user-media/addons/407142/english_us_langua 1 453872 Firefox
Viewing 25/25 records
<< < 1 of 1 pages > >>
Page size 50
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter by content type
All
Filter
Undo
Clear
www.foxtonforensics.com
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy
20 March 2021 Saturday
Type here to search
ENG
04:46 PM 20-03-2021


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 10
Browser Settings 0
Cached Files 5122
Cached Images 1236
Cached Web Pages 153
Cookies 671
Downloads 1
Email Addresses 7
Favicons 127
Form History 2
Logins 28
Searches 15
Session Tabs 52
Thumbnails 11
Website Visits 597
Cached Images
Report Preview
Last Fetched
Content Type
URL
Fetch Count
File Size (Bytes)
Web Browser
image/jpeg https://logincdn.msauth.net/16.000.28426.6/images/Backgrounds/0.jpg?x=a5dbd 1 283351 Firefox
image/png https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/t 1 259865 Firefox
image/png https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/t 1 227325 Firefox
image/png http://elearning.nkc.ac.in/pluginfile.php/22294/question/questiontext/23222/34/3 5 225985 Firefox
image/png https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/t 2 223930 Firefox
image/png https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/t 1 222991 Firefox
image/jpeg https://s.yimg.com/lo/api/res/1.2/J5dTmw3U9VukQCqxKbVxxQ--~A/Zmk9ZmlsbD 1 213583 Firefox
image/png https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/t 3 212675 Firefox
image/jpeg https://search.norton.com/images/v1/client_install/img-safe-search-bg 0 208430 Firefox
image/jpeg https://search.norton.com/images/v1/client_install/img-safe-search-bg 1 208430 Firefox
image/jpeg https://www.msn.com,https://tpc.googlesyndication.com/simgad/1153101320950 2 198935 Firefox
image/jpeg https://s.yimg.com/lo/api/res/1.2/4fVioLwZ9HJuGg2AXSUVCw--~A/Zmk9ZmlOO3 1 192015 Firefox
image/jpeg https://www.msn.com,https://tpc.googlesyndication.com/simgad/3799519700657 1 190558 Firefox
image/jpeg https://client.teamviewer.com/taf/creatives/redesign-template2016/img/tv2021-q 1 183024 Internet Explorer
image/jpeg https://www.msn.com,https://tpc.googlesyndication.com/simgad/1242759292153 1 180334 Firefox
Viewing 25/25 records
<< < 1 of 1 pages > >>
Page size 50
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter
Undo
Clear
www.foxtonforensics.com
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy
20 March 2021 Saturday
Type here to search
ENG
04:49 PM 20-03-2021


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 10
Browser Settings 0
Cached Files 5122
Cached Images 1236
Cached Web Pages 153
Cookies 671
Downloads 1
Email Addresses 7
Favicons 127
Form History 2
Logins 28
Searches 15
Session Tabs 52
Thumbnails 11
Website Visits 597
Cookies
Report Preview
Date Created URL Last Accessed Date Expires Name Content Web Browser
16-03-2021 04.52.04 .msn.com/ 16-03-2021 04.52.04 10-04-2022 05.51.32 __gads ID=ee5cec9ecfb94d3c-22d9 Firefox
16-03-2021 04.51.19 cm.mgid.com/ 16-03-2021 04.51.19 15-04-2021 05.50.46 mg_sync {"516415":1615870246} Firefox
16-03-2021 04.51.11 www.msn.com/ 16-03-2021 04.51.11 16-03-2022 04.51.11 timeZoneOffsetInMins -330 Firefox
16-03-2021 04.51.10 .c.msn.com/ 16-03-2021 04.51.10 23-03-2021 04.50.41 MR 0 Firefox
16-03-2021 04.51.10 .c.msn.com/ 16-03-2021 04.51.10 16-03-2021 05.00.41 ANONCHK 0 Firefox
16-03-2021 04.51.09 .c.bing.com/ 16-03-2021 04.51.09 23-03-2021 04.50.40 MR 0 Firefox
16-03-2021 04.51.07 .msn.com/ 16-03-2021 04.51.19 16-03-2022 04.50.49 MC1 GUID=49e96b2c455641428(Firefox
16-03-2021 04.51.07 .msn.com/ 16-03-2021 04.51.19 16-03-2021 05.20.49 MS0 803a2dc14b5a45459bb057c Firefox
16-03-2021 04.51.00 .msn.com/ 16-03-2021 04.52.13 10-04-2022 05.50.29 _EDGE_V 1 Firefox
16-03-2021 04.51.00 .msn.com/ 16-03-2021 04.52.13 10-04-2022 05.50.41 MUID 2F13A437A96062BB0B13ABI Firefox
16-03-2021 04.50.58 .amazon.fr/ 16-03-2021 04.50.58 16-03-2022 04.50.28 ubid-acbfr 259-0676198-8539827 Firefox
16-03-2021 04.50.57 .msn.com/ 16-03-2021 04.52.13 16-03-2022 04.50.29 PreferencesMsn eyJlb21IUGFnZSI6eyJTdHJpc Firefox
16-03-2021 04.50.57 .msn.com/ 16-03-2021 04.52.13 16-03-2022 04.50.29 marketPref en-in Firefox
16-03-2021 04.50.57 www.msn.com/ 16-03-2021 04.51.06 16-09-2022 05.50.36 cobrand acer17win10.msn.com Firefox
16-03-2021 04.50.57 .amazon.com/ 16-03-2021 04.51.28 01-01-2036 08.00.01 session-token 8H7hkH+Pfq11N4b0d2l9Zkl Firefox
18-02-2021 04.29.22 .chrome.google.com/ 18-02-2021 04.29.22 18-02-2021 04.59.22 __utmb Chrome
18-02-2021 04.29.06 .chrome.google.com/ 18-02-2021 04.29.06 18-02-2021 04.39.06 __utmt Chrome
18-02-2021 04.29.05 .chrome.google.com/ 18-02-2021 04.29.22 18-02-2023 04.29.22 __utma Chrome
18-02-2021 04.29.05 .chrome.google.com/ 18-02-2021 04.29.22 19-08-2021 17.29.22 __utmz Chrome
18-02-2021 04.29.03 .google.com/ 18-02-2021 04.29.03 20-08-2021 05.29.03 NID Chrome
10-02-2021 04.09.41 ogs.google.com/ 10-02-2021 04.09.41 12-03-2021 04.09.41 OTZ 5843770_34_34__34_ Firefox
10-02-2021 04.06.21 meet.google.com/ 10-02-2021 04.08.39 12-03-2021 04.06.21 OTZ 5843766_34_34__34_ Firefox
10-02-2021 04.06.16 .youtube.com/ 16-03-2021 04.51.41 10-02-2023 04.06.40 SID 6gevnJ3NlxXRS-N-pEo5oeE(Firefox
10-02-2021 04.06.16 .youtube.com/ 16-03-2021 04.51.41 10-02-2023 04.06.40 __Secure-3PSID 6gevnJ3NlxXRS-N-pEo5oeE(Firefox
10-02-2021 04.06.16 .youtube.com/ 16-03-2021 04.51.41 10-02-2023 04.06.40 HSID AY36-9zkyFfTeff5d Firefox
Viewing 25/25 records
<< < 1 of 1 pages > >>
Page size 50
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter Undo Clear
www.foxtonforensics.com
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy
20 March 2021 Saturday
Type here to search
ENG 04:51 PM 20-03-2021


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 10
Browser Settings 0
Cached Files 5122
Cached Images 1236
Cached Web Pages 153
Cookies 671
Downloads 1
Email Addresses 7
Favicons 127
Form History 2
Logins 28
Searches 15
Session Tabs 52
Thumbnails 11
Website Visits 597
Cookies
Report Preview
Save As
This PC > Desktop > tycs sem6 > cyber forensics
Search cyber forensics
Organize New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
local (C:)
New Volume (D:)
Name Status Date modified Type
Capture 20-03-2021 04:34 PM File folder
demo 20-01-2021 10:47 AM File folder
kuldeep patel 20-03-2021 01:06 PM File folder
CF - PRACT 5-10 07-02-2021 12:04 PM PDF File
Cyberforensics - 2020 - Practical 20-01-2021 10:26 AM PDF File
email forencis 10-03-2021 08:45 AM PDF File
E-Mail Forensics (574) 10-03-2021 09:02 AM PDF File
File name: History Report_574
Save as type: PDF documents (.pdf)
Hide Folders
Save Cancel
Viewing 25/25 records
<< < 1 of 1 pages > >>
Page size 50
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter Undo Clear
www.foxtonforensics.com
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy
20 March 2021 Saturday
Type here to search
ENG 04:52 PM 20-03-2021



Web Browser History Report

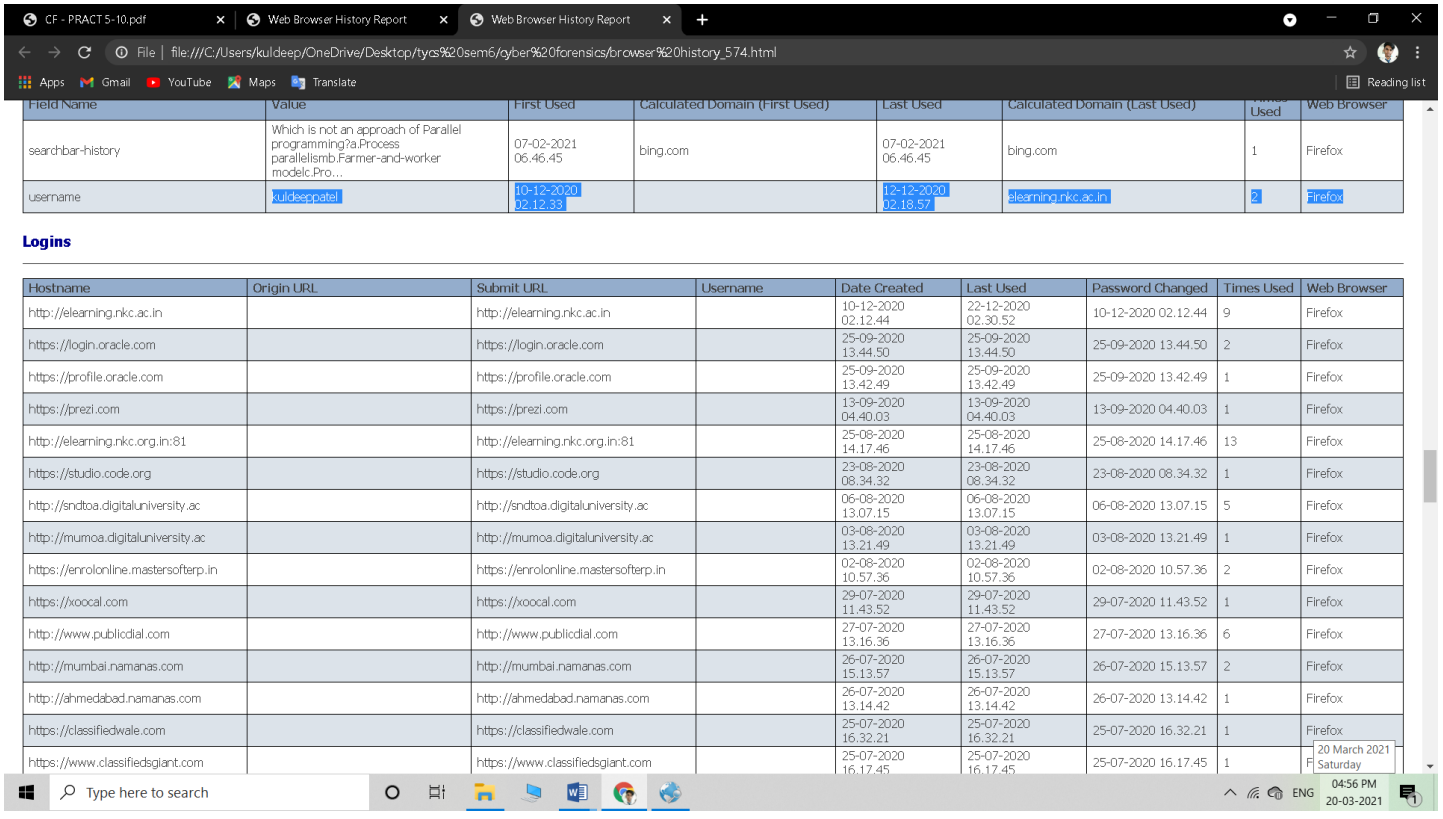
Created: 20-03-2021 16.55
Created using: Browser History Examiner v1.13
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy

Bookmarks

Date Added	Last Modified	Title	URL	Web Browser
03-02-2020 15.54.58	03-02-2020 15.54.58	Agoda	https://s3.amazonaws.com/amundsen/redirect/19q2/agoda.html?utm_source=win32&utm_medium=favorite	Firefox
03-02-2020 15.54.58	03-02-2020 15.54.58	Getting Started	https://www.mozilla.org/en-US/firefox/central/	Firefox
03-02-2020 15.54.58	03-02-2020 15.54.58	Help and Tutorials	https://support.mozilla.org/en-US/products/firefox	Firefox
03-02-2020 15.54.58	03-02-2020 15.54.58	Customize Firefox	https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=fire...	Firefox
03-02-2020 15.54.58	03-02-2020 15.54.58	Get Involved	https://www.mozilla.org/en-US/contribute/	Firefox
03-02-2020 15.54.58	03-02-2020 15.54.58	About Us	https://www.mozilla.org/en-US/about/	Firefox
		Bing	http://go.microsoft.com/fwlink/p/?LinkId=255142	Internet Explorer
		Acer	http://www.acer.com	Internet Explorer
		Agoda	https://s3.amazonaws.com/amundsen/redirect/19q2/agoda.html?utm_source=win32&utm_medium=favorite	Internet Explorer
		Agoda	https://s3.amazonaws.com/amundsen/redirect/19q2/agoda.html?utm_source=win32&utm_medium=favorite	Edge

Cached Files

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
	application/octet-stream	https://download-installer.cdn.mozilla.net/pub/firefox/releases/84.0/update/win64/en-US/firefox-83.0...	1	16409690	Firefox
	application/octet-stream	http://download.cdn.mozilla.net/pub/firefox/releases/73.0.1/update/win64/en-US/firefox-72.0.2-73.0.1...	1	13664061	Firefox
	application/zip	https://r8---sn-ci5gup-cvhr.gvt1.com/edgedl/widevine-cdm/4.10.1582.2-win-x64.zip?cms_redirect=yes&am...	1	5097580	Firefox
	application/zip	https://r4---sn-ci5gup-cvhr.gvt1.com/edgedl/widevine-cdm/4.10.1440.19-win-x64.zip?cms_redirect=yes&a...	1	4753555	Firefox
	application/javascript	http://elearning.nkc.ac.in/lib/requirejs.php/1604566322/core/firs	128	2000420	F



Field Name	Value	First Used	Calculated Domain (First Used)	Last Used	Calculated Domain (Last Used)	Used	Web Browser
searchbar-history	Which is not an approach of Parallel programming?a.Process parallelismb.Farmer-and-worker modelc.Pro...	07-02-2021 06.46.45	bing.com	07-02-2021 06.46.45	bing.com	1	Firefox
username	kuldeeppatel	10-12-2020 02.12.33		12-12-2020 02.18.57	elearning.nkc.ac.in	2	Firefox

Logins

Hostname	Origin URL	Submit URL	Username	Date Created	Last Used	Password Changed	Times Used	Web Browser
http://elearning.nkc.ac.in		http://elearning.nkc.ac.in		10-12-2020 02.12.44	22-12-2020 02.30.52	10-12-2020 02.12.44	9	Firefox
https://login.oracle.com		https://login.oracle.com		25-09-2020 13.44.50	25-09-2020 13.44.50	25-09-2020 13.44.50	2	Firefox
https://profile.oracle.com		https://profile.oracle.com		25-09-2020 13.42.49	25-09-2020 13.42.49	25-09-2020 13.42.49	1	Firefox
https://prezi.com		https://prezi.com		13-09-2020 04.40.03	13-09-2020 04.40.03	13-09-2020 04.40.03	1	Firefox
http://elearning.nkc.org.in:81		http://elearning.nkc.org.in:81		25-08-2020 14.17.46	25-08-2020 14.17.46	25-08-2020 14.17.46	13	Firefox
https://studio.code.org		https://studio.code.org		23-08-2020 08.34.32	23-08-2020 08.34.32	23-08-2020 08.34.32	1	Firefox
http://sndtoa.digitaluniversity.ac		http://sndtoa.digitaluniversity.ac		06-08-2020 13.07.15	06-08-2020 13.07.15	06-08-2020 13.07.15	5	Firefox
http://mumoa.digitaluniversity.ac		http://mumoa.digitaluniversity.ac		03-08-2020 13.21.49	03-08-2020 13.21.49	03-08-2020 13.21.49	1	Firefox
https://enrolonline.mastersofterp.in		https://enrolonline.mastersofterp.in		02-08-2020 10.57.36	02-08-2020 10.57.36	02-08-2020 10.57.36	2	Firefox
https://xoocal.com		https://xoocal.com		29-07-2020 11.43.52	29-07-2020 11.43.52	29-07-2020 11.43.52	1	Firefox
http://www.publicdial.com		http://www.publicdial.com		27-07-2020 13.16.36	27-07-2020 13.16.36	27-07-2020 13.16.36	6	Firefox
http://mumbai.namanas.com		http://mumbai.namanas.com		26-07-2020 15.13.57	26-07-2020 15.13.57	26-07-2020 15.13.57	2	Firefox
http://ahmedabad.namanas.com		http://ahmedabad.namanas.com		26-07-2020 13.14.42	26-07-2020 13.14.42	26-07-2020 13.14.42	1	Firefox
https://classifiedwale.com		https://classifiedwale.com		25-07-2020 16.32.21	25-07-2020 16.32.21	25-07-2020 16.32.21	1	Firefox
https://www.classifiedsgiant.com		https://www.classifiedsgiant.com		25-07-2020 16.17.45	25-07-2020 16.17.45	25-07-2020 16.17.45	1	F