Digital Forensics Incidence response

CSUDH

CALIFORNIA STATE UNIVERSITY, DOMINGUEZ HILLS

By:

Yahya Sayeed

Master of Science in Cybersecurity

CYB590 – Graduate Project

Fall - 2023

Abstract

- Defensive strategies to avoid a cybersecurity incidents.[1]
- Cyberattacks are happening with more sophistication and is inevitable.
- Incidence Response stops, contains the attack and gets operations back to normal as soon as possible.
- Traditional incidence response lack few capabilities which makes way for

  Digital Forensics Incidence Response (DFIR).

- Delivers deeper understanding through a comprehensive and intricate forensic process.
- DFIR specialists gather and inspect a wealth of information to determine:
  - Who attacked them?[1] How they got in? [1]
  - What are the exact steps taken by attackers to compromise their systems? [1]
  - What the organization should do to close those security gaps.[1]

The aim of this project is to focus on various areas where the evidence can be acquired analyzed using digital forensics tools and techniques to find the root cause analysis behind an incident.

Introduction

Acquisition

Preserve, Analyze & Recover[1]

Report findings

- Speed is critical.
- Computers and devices in a network are continuously producing data that may be crucial to an investigation.
- Over time, the risk that this data is deleted, overwritten, or otherwise altered increases.[1]
- Forensic investigators need to move quickly to ensure they capture all this information before it's lost.

Background

Acquisition

- Duplicate copy of media.
- Forensic images.

Analysis

- De-duplication.
- OCR.
- Index.
- Searching.

Reporting

- Findings.
- Conclusions.

Figure1: Key Steps of Digital Forensics[1]

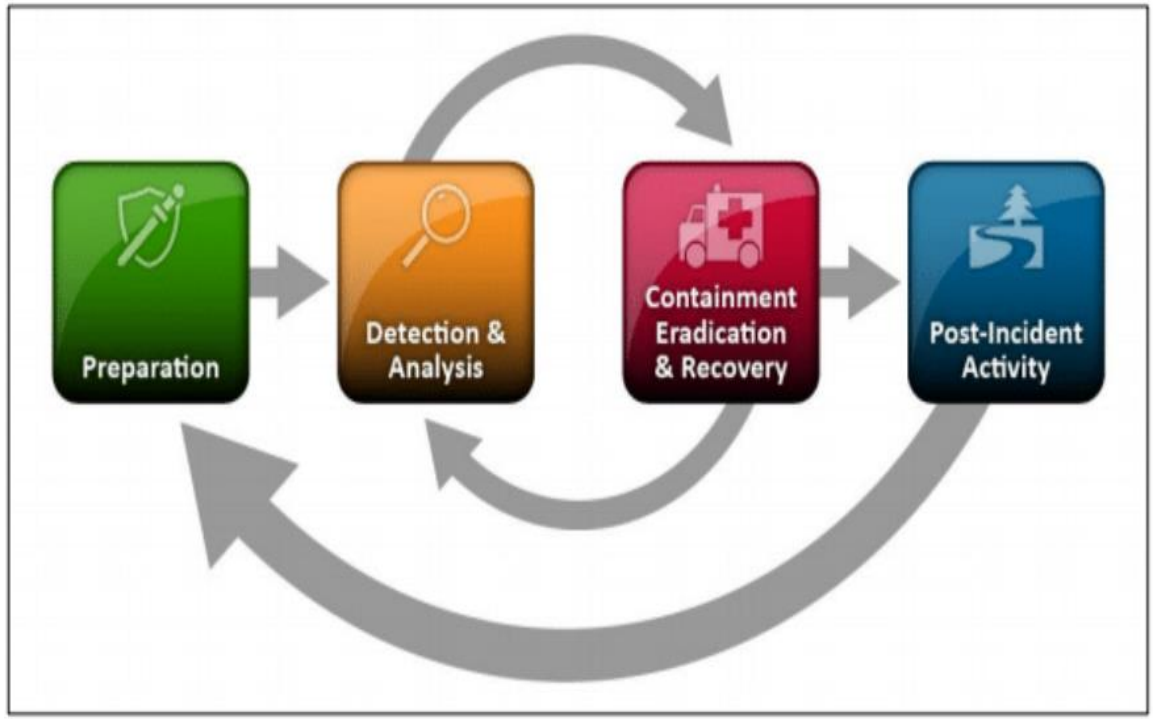
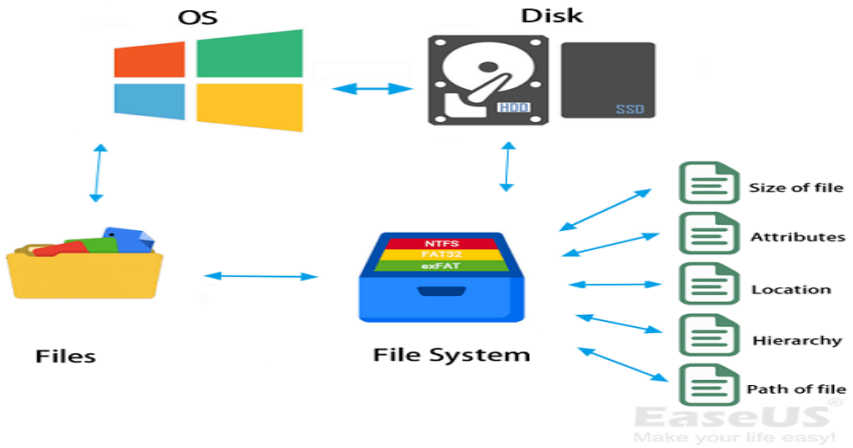


Figure2: Steps in Incidence Response[2,3,5]

NetWitness Investigator[6] Proposed Method

Wireshark[7]



Network Analysis[4]

A sample packet capture is taken and analyzed for any cyber-attacks.

In-memory Analysis[4]

The memory analysis is performed on the compromised live machine to perform bit by bit physical acquisition from the entire hard-drive.

Media Analysis[4]

Captures the logical memory of the drive which means only the allocated spaces of the drive.

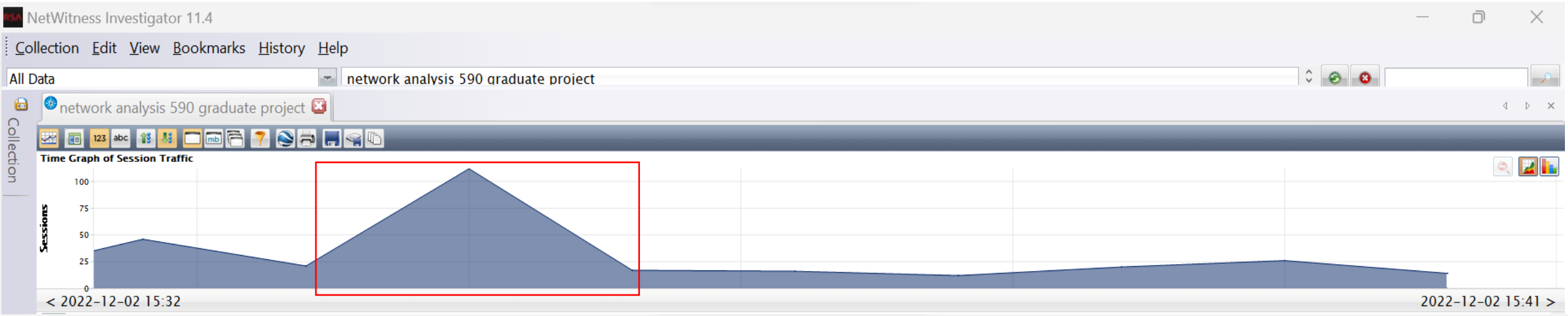
Access Data FTK[8]

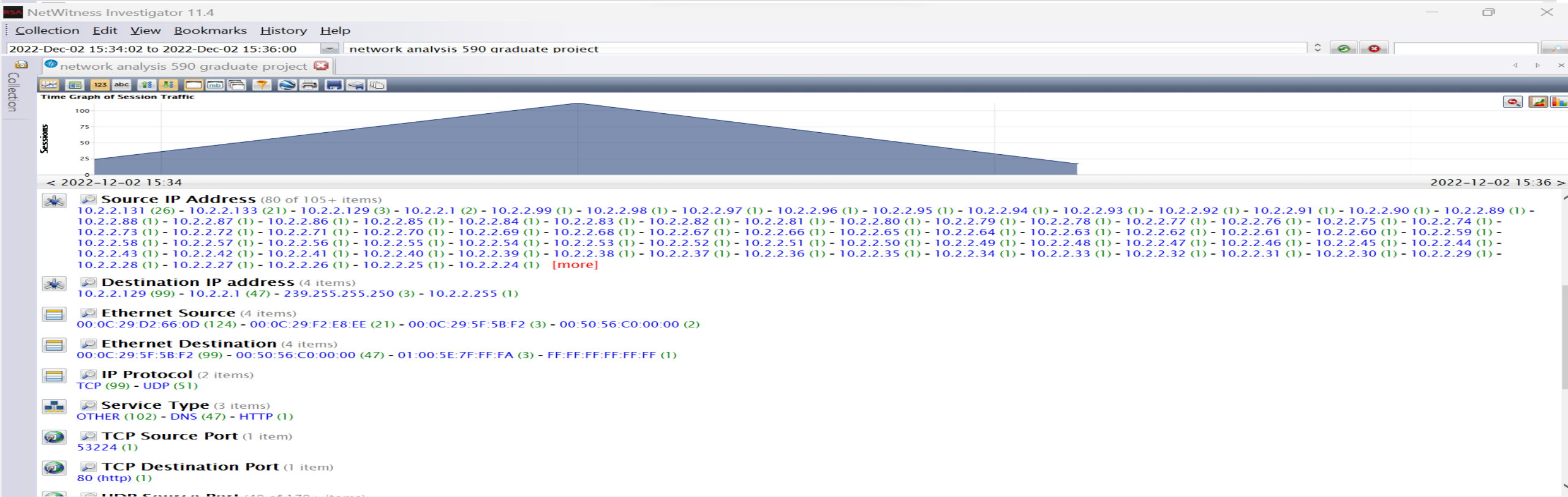
Paraben's E3[9]

Embedded/Hardware Analysis[4]

Acquisition of data from a smartphone to analyze the data contacts, SMS, call logs, applications installed on the mobile device.

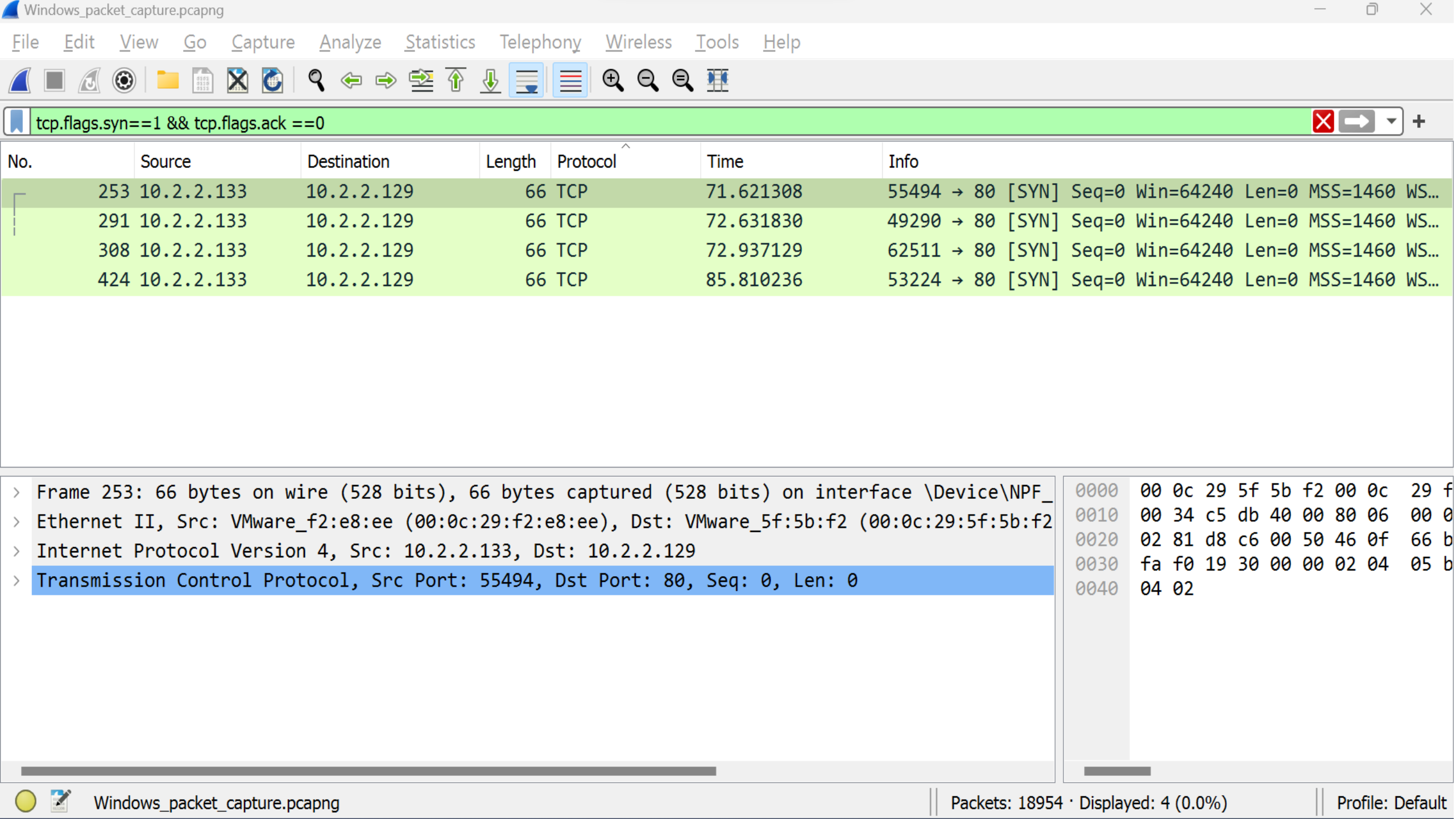
Implementation

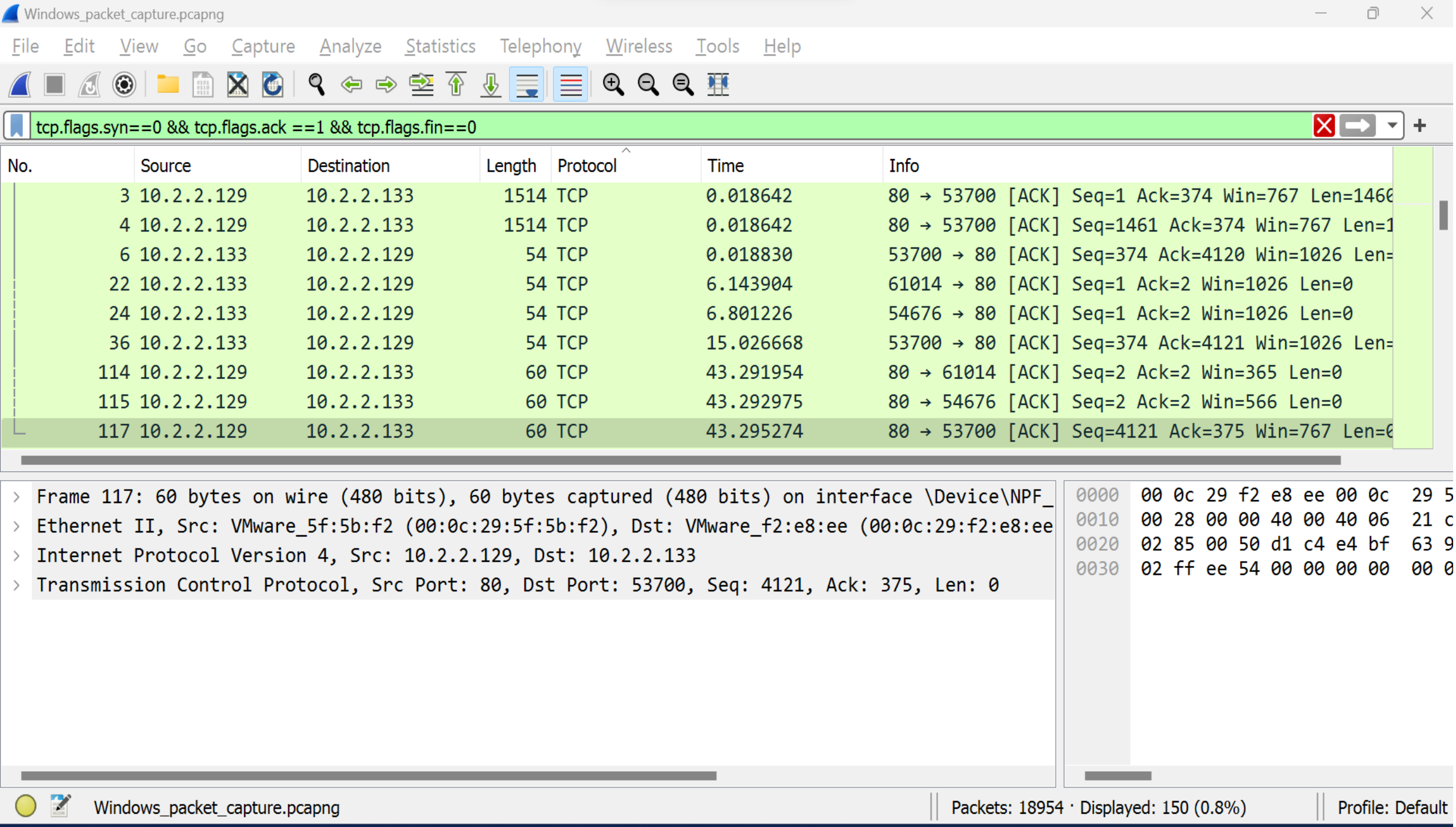


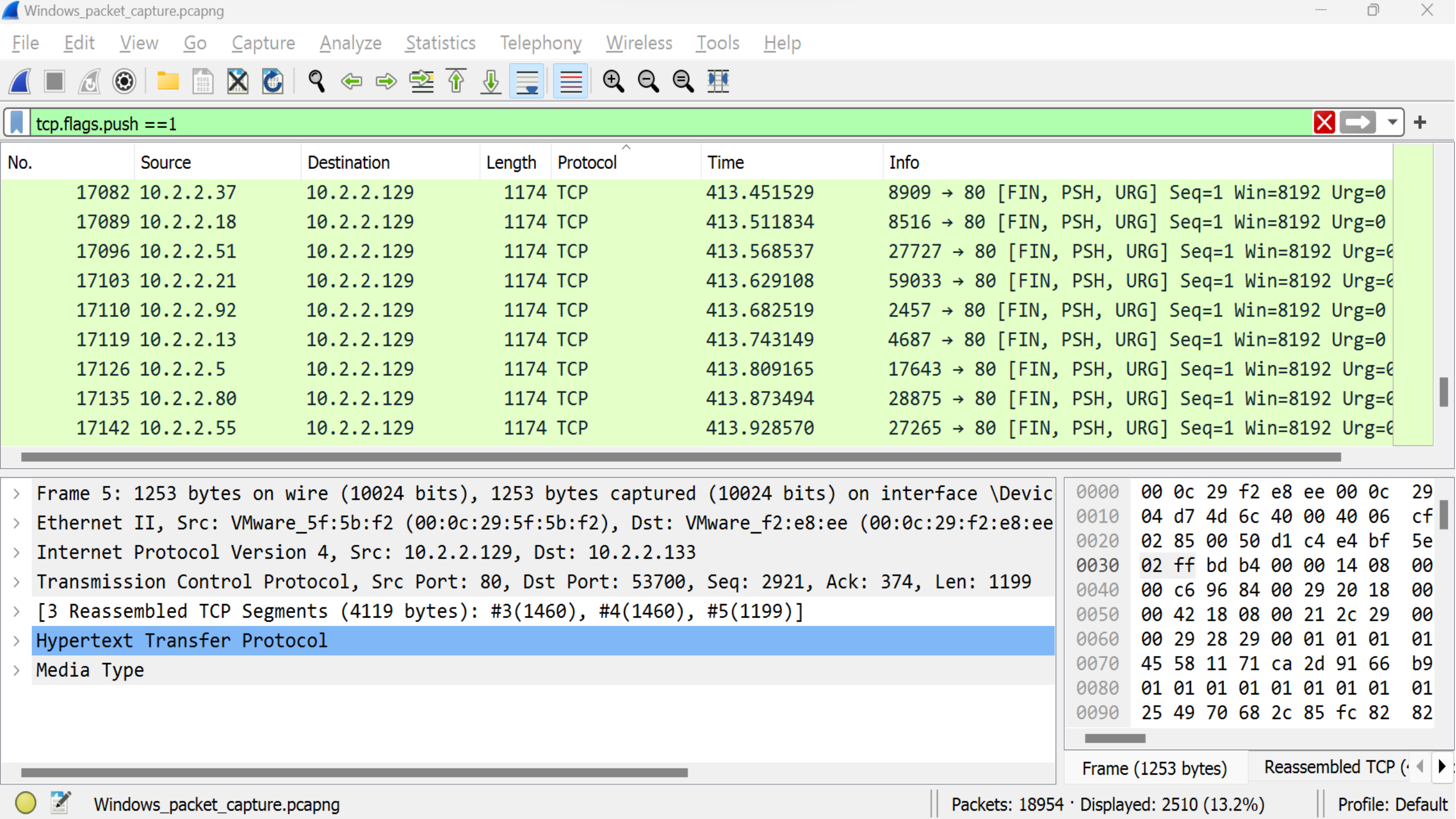


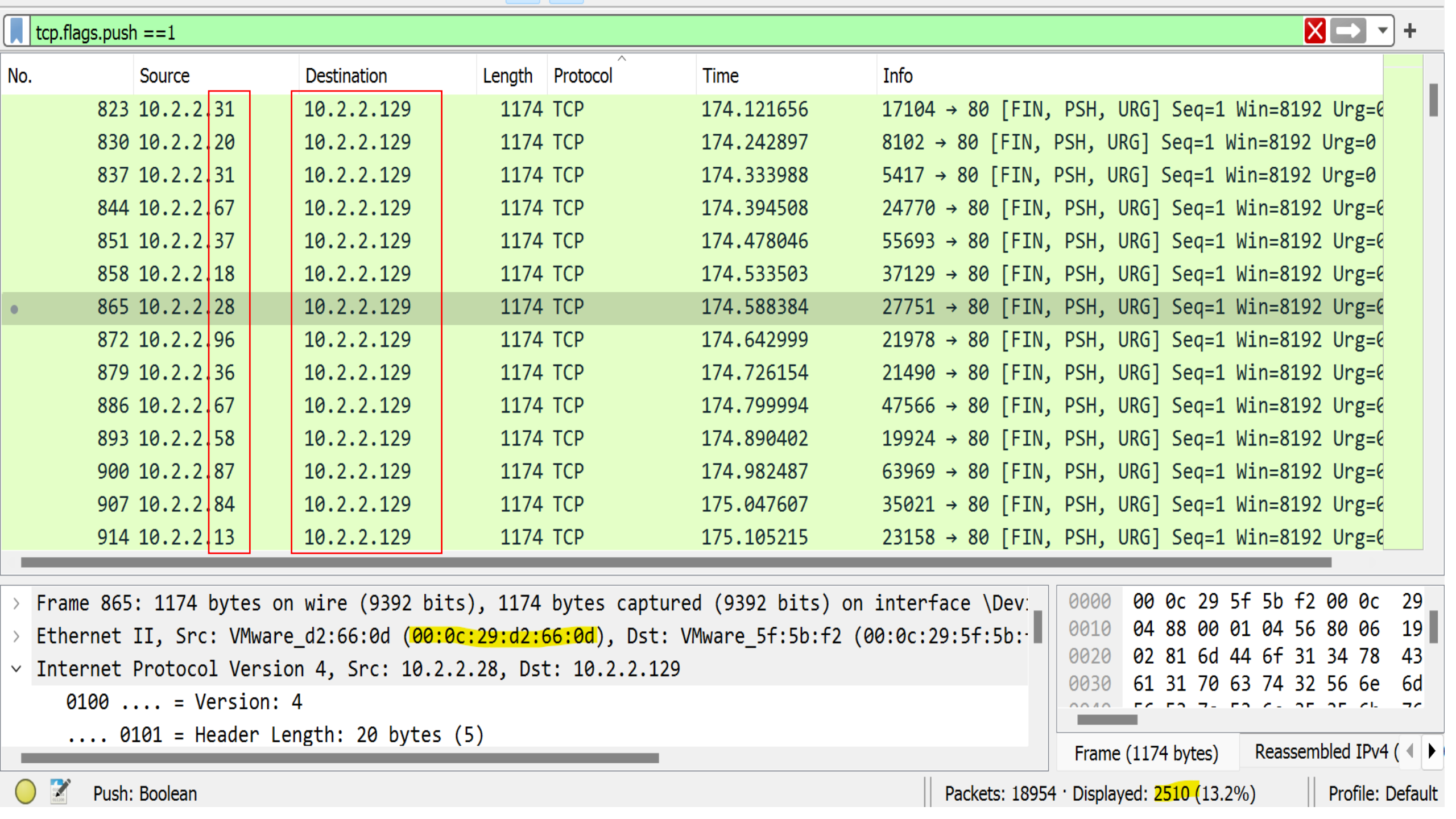
	Time	Service	Size	Events
 View	2022-Dec-02 15:35:37	IP / TCP / OTHER	190.33 KB	00:0C:29:D2:66:0D -> 00:0C:29:5F:5B:F2 10.2.2.84 -> 10.2.2.129 payload: 190380 medium: Ethernet streams: 1 packets: 133 lifetime: 245 mcbc.req: 3572 mcb.req: 48 ubc.req: 114 entropy.req: 5962 payload.req: 190380
 View	2022-Dec-02 15:35:37	IP / TCP / OTHER	290.50 KB	00:0C:29:D2:66:0D -> 00:0C:29:5F:5B:F2 10.2.2.13 -> 10.2.2.129 payload: 290580 medium: Ethernet streams: 1 packets: 203 lifetime: 239 mcbc.req: 5308 mcb.req: 79 ubc.req: 133 entropy.req: 5962 payload.req: 290580
 View	2022-Dec-02 15:35:37	IP / TCP / OTHER	340.59 KB	00:0C:29:D2:66:0D -> 00:0C:29:5F:5B:F2 10.2.2.8 -> 10.2.2.129 payload: 340680 medium: Ethernet streams: 1 packets: 238 lifetime: 247 mcbc.req: 6834 mcb.req: 121 ubc.req: 147 entropy.req: 5961 payload.req: 340680
	2022-Dec-02 15:35:37	IP / TCP / OTHER	220.38 KB	00:0C:29:D2:66:0D -> 00:0C:29:5F:5B:F2

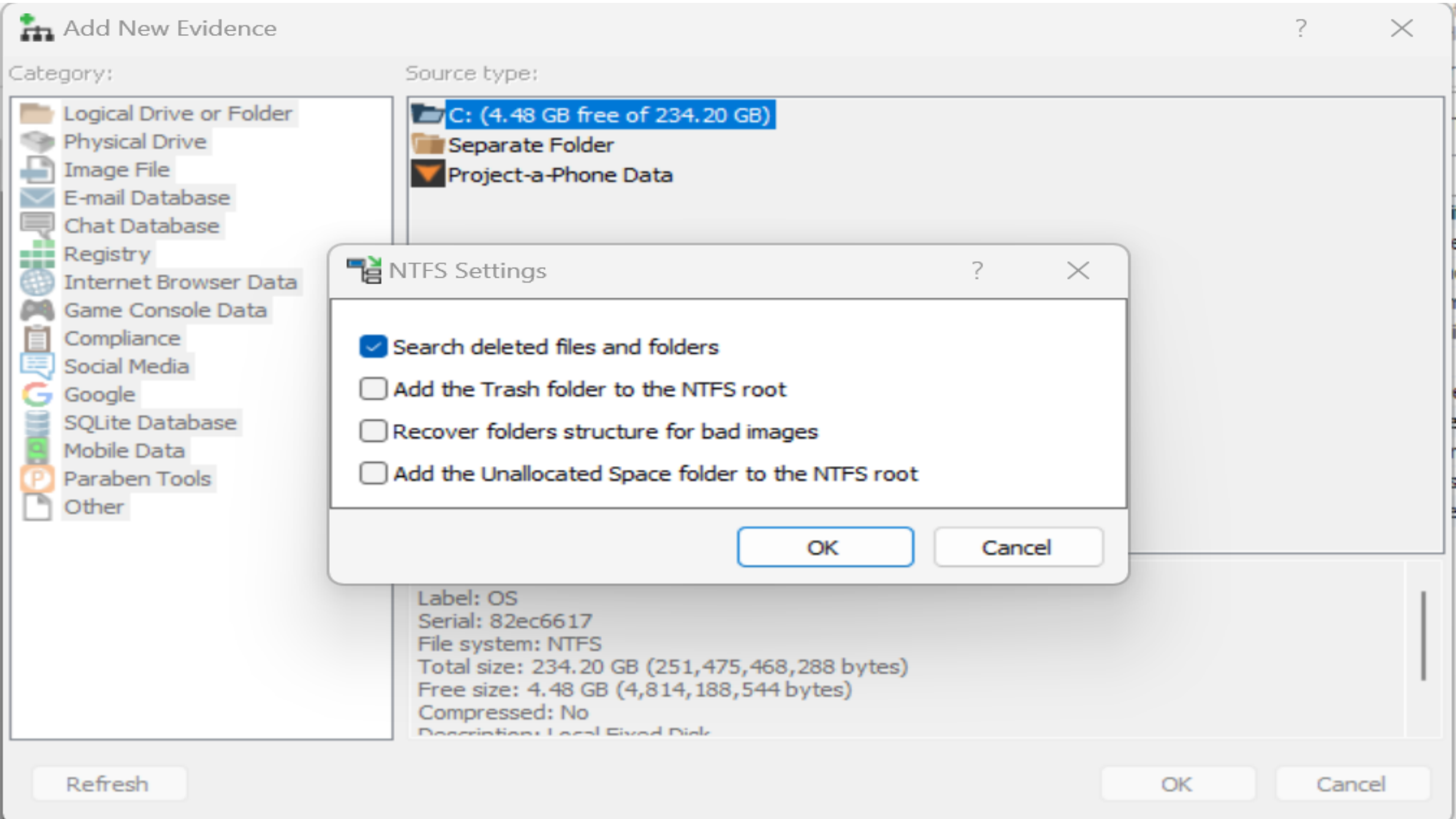
Displaying 21 – 40 of 99

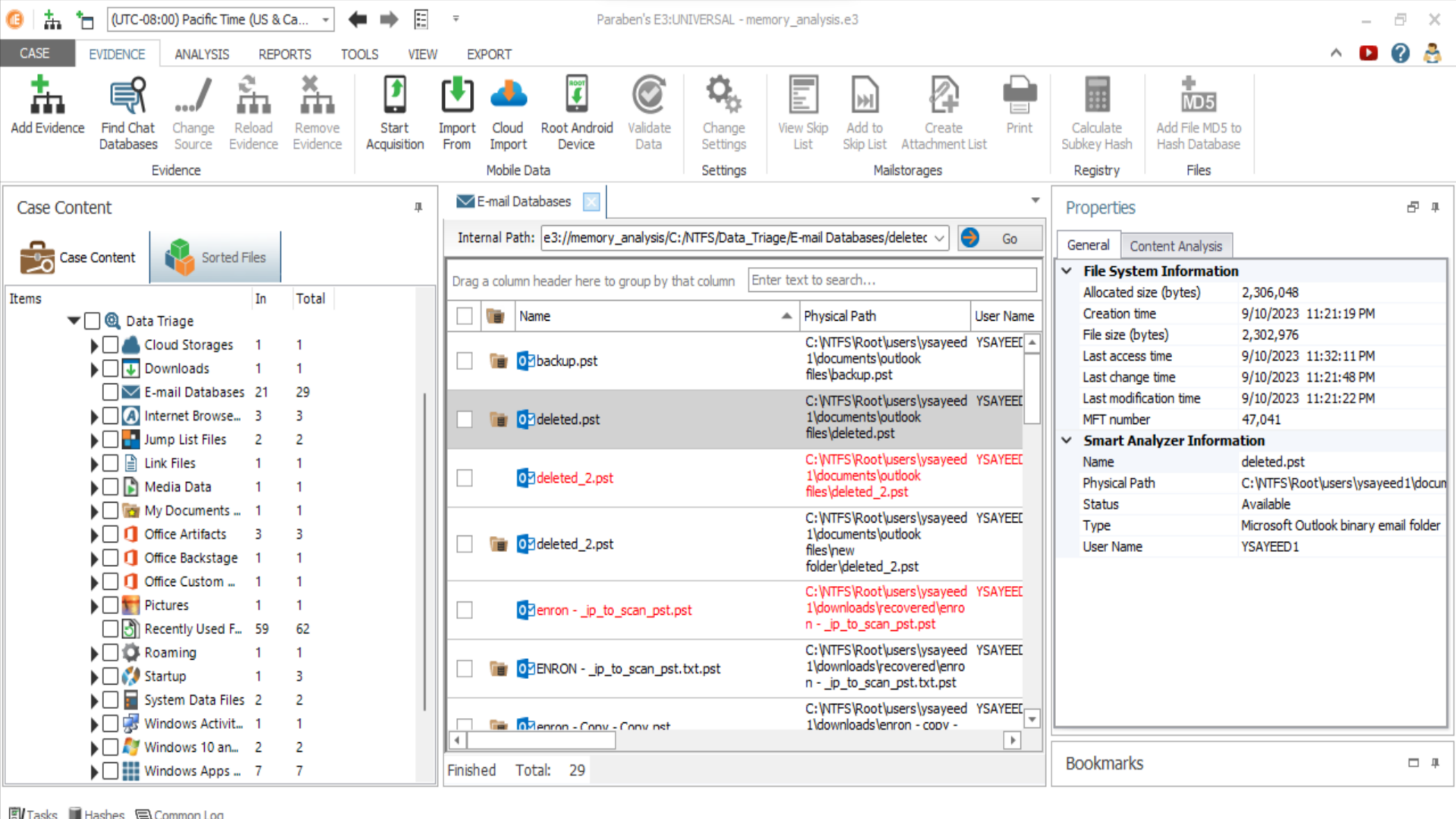

Windows_packet_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==1 && tcp.flags.ack ==0
No. Source Destination Length Protocol Time Info
253 10.2.2.133 10.2.2.129 66 TCP 71.621308 55494 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS…
291 10.2.2.133 10.2.2.129 66 TCP 72.631830 49290 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS…
308 10.2.2.133 10.2.2.129 66 TCP 72.937129 62511 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS…
424 10.2.2.133 10.2.2.129 66 TCP 85.810236 53224 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS…
Frame 253: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_
Ethernet II, Src: VMware_f2:e8:ee (00:0c:29:f2:e8:ee), Dst: VMware_5f:5b:f2 (00:0c:29:5f:5b:f2
Internet Protocol Version 4, Src: 10.2.2.133, Dst: 10.2.2.129
Transmission Control Protocol, Src Port: 55494, Dst Port: 80, Seq: 0, Len: 0
0000 00 0c 29 5f 5b f2 00 0c 29 f
0010 00 34 c5 db 40 00 80 06 00 0
0020 02 81 d8 c6 00 50 46 0f 66 b
0030 fa f0 19 30 00 00 02 04 05 b
0040 04 02
Windows_packet_capture.pcapng
Packets: 18954 · Displayed: 4 (0.0%)
Profile: Default


Windows_packet_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==0 && tcp.flags.ack ==1 && tcp.flags.fin==0
No. Source Destination Length Protocol Time Info
3 10.2.2.129 10.2.2.133 1514 TCP 0.018642 80 → 53700 [ACK] Seq=1 Ack=374 Win=767 Len=1460
4 10.2.2.129 10.2.2.133 1514 TCP 0.018642 80 → 53700 [ACK] Seq=1461 Ack=374 Win=767 Len=1
6 10.2.2.133 10.2.2.129 54 TCP 0.018830 53700 → 80 [ACK] Seq=374 Ack=4120 Win=1026 Len=
22 10.2.2.133 10.2.2.129 54 TCP 6.143904 61014 → 80 [ACK] Seq=1 Ack=2 Win=1026 Len=0
24 10.2.2.133 10.2.2.129 54 TCP 6.801226 54676 → 80 [ACK] Seq=1 Ack=2 Win=1026 Len=0
36 10.2.2.133 10.2.2.129 54 TCP 15.026668 53700 → 80 [ACK] Seq=374 Ack=4121 Win=1026 Len=
114 10.2.2.129 10.2.2.133 60 TCP 43.291954 80 → 61014 [ACK] Seq=2 Ack=2 Win=365 Len=0
115 10.2.2.129 10.2.2.133 60 TCP 43.292975 80 → 54676 [ACK] Seq=2 Ack=2 Win=566 Len=0
117 10.2.2.129 10.2.2.133 60 TCP 43.295274 80 → 53700 [ACK] Seq=4121 Ack=375 Win=767 Len=0
Frame 117: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_
Ethernet II, Src: VMware_5f:5b:f2 (00:0c:29:5f:5b:f2), Dst: VMware_f2:e8:ee (00:0c:29:f2:e8:ee
Internet Protocol Version 4, Src: 10.2.2.129, Dst: 10.2.2.133
Transmission Control Protocol, Src Port: 80, Dst Port: 53700, Seq: 4121, Ack: 375, Len: 0
0000 00 0c 29 f2 e8 ee 00 0c 29 5
0010 00 28 00 00 40 00 40 06 21 c
0020 02 85 00 50 d1 c4 e4 bf 63 9
0030 02 ff ee 54 00 00 00 00 00 0
Windows_packet_capture.pcapng
Packets: 18954 · Displayed: 150 (0.8%)
Profile: Default


Windows_packet_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.push ==1
No. Source Destination Length Protocol Time Info
17082 10.2.2.37 10.2.2.129 1174 TCP 413.451529 8909 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
17089 10.2.2.18 10.2.2.129 1174 TCP 413.511834 8516 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
17096 10.2.2.51 10.2.2.129 1174 TCP 413.568537 27727 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
17103 10.2.2.21 10.2.2.129 1174 TCP 413.629108 59033 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
17110 10.2.2.92 10.2.2.129 1174 TCP 413.682519 2457 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
17119 10.2.2.13 10.2.2.129 1174 TCP 413.743149 4687 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
17126 10.2.2.5 10.2.2.129 1174 TCP 413.809165 17643 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
17135 10.2.2.80 10.2.2.129 1174 TCP 413.873494 28875 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
17142 10.2.2.55 10.2.2.129 1174 TCP 413.928570 27265 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
Frame 5: 1253 bytes on wire (10024 bits), 1253 bytes captured (10024 bits) on interface \Devic
Ethernet II, Src: VMware_5f:5b:f2 (00:0c:29:5f:5b:f2), Dst: VMware_f2:e8:ee (00:0c:29:f2:e8:ee
Internet Protocol Version 4, Src: 10.2.2.129, Dst: 10.2.2.133
Transmission Control Protocol, Src Port: 80, Dst Port: 53700, Seq: 2921, Ack: 374, Len: 1199
[3 Reassembled TCP Segments (4119 bytes): #3(1460), #4(1460), #5(1199)]
Hypertext Transfer Protocol
Media Type
0000 00 0c 29 f2 e8 ee 00 0c 29
0010 04 d7 4d 6c 40 00 40 06 cf
0020 02 85 00 50 d1 c4 e4 bf 5e
0030 02 ff bd b4 00 00 14 08 00
0040 00 c6 96 84 00 29 20 18 00
0050 00 42 18 08 00 21 2c 29 00
0060 00 29 28 29 00 01 01 01 01
0070 45 58 11 71 ca 2d 91 66 b9
0080 01 01 01 01 01 01 01 01 01
0090 25 49 70 68 2c 85 fc 82 82
Frame (1253 bytes)
Reassembled TCP (
Windows_packet_capture.pcapng
Packets: 18954 · Displayed: 2510 (13.2%)
Profile: Default


tcp.flags.push ==1
No. Source Destination Length Protocol Time Info
823 10.2.2.31 10.2.2.129 1174 TCP 174.121656 17104 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
830 10.2.2.20 10.2.2.129 1174 TCP 174.242897 8102 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
837 10.2.2.31 10.2.2.129 1174 TCP 174.333988 5417 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
844 10.2.2.67 10.2.2.129 1174 TCP 174.394508 24770 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
851 10.2.2.37 10.2.2.129 1174 TCP 174.478046 55693 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
858 10.2.2.18 10.2.2.129 1174 TCP 174.533503 37129 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
865 10.2.2.28 10.2.2.129 1174 TCP 174.588384 27751 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
872 10.2.2.96 10.2.2.129 1174 TCP 174.642999 21978 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
879 10.2.2.36 10.2.2.129 1174 TCP 174.726154 21490 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
886 10.2.2.67 10.2.2.129 1174 TCP 174.799994 47566 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
893 10.2.2.58 10.2.2.129 1174 TCP 174.890402 19924 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
900 10.2.2.87 10.2.2.129 1174 TCP 174.982487 63969 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
907 10.2.2.84 10.2.2.129 1174 TCP 175.047607 35021 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
914 10.2.2.13 10.2.2.129 1174 TCP 175.105215 23158 → 80 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0
Frame 865: 1174 bytes on wire (9392 bits), 1174 bytes captured (9392 bits) on interface \Dev
Ethernet II, Src: VMware_d2:66:0d (00:0c:29:d2:66:0d), Dst: VMware_5f:5b:f2 (00:0c:29:5f:5b:
Internet Protocol Version 4, Src: 10.2.2.28, Dst: 10.2.2.129
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
0000 00 0c 29 5f 5b f2 00 0c 29
0010 04 88 00 01 04 56 80 06 19
0020 02 81 6d 44 6f 31 34 78 43
0030 61 31 70 63 74 32 56 6e 6d
Frame (1174 bytes)
Reassembled IPv4 (
Push: Boolean
Packets: 18954 · Displayed: 2510 (13.2%)
Profile: Default


Add New Evidence
Category:
Source type:
Logical Drive or Folder
Physical Drive
Image File
E-mail Database
Chat Database
Registry
Internet Browser Data
Game Console Data
Compliance
Social Media
Google
SQLite Database
Mobile Data
Paraben Tools
Other
C: (4.48 GB free of 234.20 GB)
Separate Folder
Project-a-Phone Data
NTFS Settings
Search deleted files and folders
Add the Trash folder to the NTFS root
Recover folders structure for bad images
Add the Unallocated Space folder to the NTFS root
OK
Cancel
Label: OS
Serial: 82ec6617
File system: NTFS
Total size: 234.20 GB (251,475,468,288 bytes)
Free size: 4.48 GB (4,814,188,544 bytes)
Compressed: No
Refresh
OK
Cancel


(UTC-08:00) Pacific Time (US & Ca...
Paraben's E3:UNIVERSAL - memory_analysis.e3
CASE
EVIDENCE
ANALYSIS
REPORTS
TOOLS
VIEW
EXPORT
Add Evidence
Find Chat Databases
Change Source
Reload Evidence
Remove Evidence
Evidence
Start Acquisition
Import From
Cloud Import
Root Android Device
Validate Data
Mobile Data
Change Settings
Settings
View Skip List
Add to Skip List
Create Attachment List
Print
Mailstorages
Calculate Subkey Hash
Registry
Add File MD5 to Hash Database
Files
Case Content
Case Content
Sorted Files
Items
In
Total
Data Triage
Cloud Storages 1 1
Downloads 1 1
E-mail Databases 21 29
Internet Browse... 3 3
Jump List Files 2 2
Link Files 1 1
Media Data 1 1
My Documents ... 1 1
Office Artifacts 3 3
Office Backstage 1 1
Office Custom ... 1 1
Pictures 1 1
Recently Used F... 59 62
Roaming 1 1
Startup 1 3
System Data Files 2 2
Windows Activit... 1 1
Windows 10 an... 2 2
Windows Apps ... 7 7
E-mail Databases
Internal Path: e3://memory_analysis/C:/NTFS/Data_Triage/E-mail Databases/deletec
Go
Drag a column header here to group by that column
Enter text to search...
Name
Physical Path
User Name
backup.pst C:\NTFS\Root\users\ysayeed1\documents\outlook files\backup.pst YSAYEED
deleted.pst C:\NTFS\Root\users\ysayeed1\documents\outlook files\deleted.pst YSAYEED
deleted_2.pst C:\NTFS\Root\users\ysayeed1\documents\outlook files\deleted_2.pst YSAYEED
deleted_2.pst C:\NTFS\Root\users\ysayeed1\documents\outlook files\new folder\deleted_2.pst YSAYEED
enron - _ip_to_scan_pst.pst C:\NTFS\Root\users\ysayeed1\downloads\recovered\enron - _ip_to_scan_pst.pst YSAYEED
ENRON - _ip_to_scan_pst.txt.pst C:\NTFS\Root\users\ysayeed1\downloads\recovered\enron - _ip_to_scan_pst.txt.pst YSAYEED
enron - Copy - Copy.pst C:\NTFS\Root\users\ysayeed1\downloads\enron - copy - YSAYEED
Finished Total: 29
Properties
General
Content Analysis
File System Information
Allocated size (bytes) 2,306,048
Creation time 9/10/2023 11:21:19 PM
File size (bytes) 2,302,976
Last access time 9/10/2023 11:32:11 PM
Last change time 9/10/2023 11:21:48 PM
Last modification time 9/10/2023 11:21:22 PM
MFT number 47,041
Smart Analyzer Information
Name deleted.pst
Physical Path C:\NTFS\Root\users\ysayeed1\docun
Status Available
Type Microsoft Outlook binary email folder
User Name YSAYEED1
Bookmarks
Tasks
Hashes
Common Log

AccessData FTK Imager 4.7.1.2

File View Mode Help

Properties

Create Image

Select Image Destination

Image Destination Folder

C:\Users\ysayeed1\Documents\media_analysis_590

Browse

Image Filename (Excluding Extension)

media_analysis

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment

1500

Compression (0=None, 1=Fastest, ..., 9=Smallest)

6

Use AD Encryption

Filter by File Owner

< Back Finish Cancel Help

Start Cancel

Properties Hex Value Interpreter Custom Content Sources

For User Guide, press F1

AccessData FTK Imager 4.7.1.2

File View Mode Help

Properties

Creating Image...

Image Source: C:\Users\ysayeed1\Documents\590_graduate_project

Destination: C:\Users\ysayeed1\Documents\media_analysis_590\media_a

Status: Creating image...

Progress

Elapsed time: 0:00:09

Estimated time left:

Cancel

Properties | Hex Value Interpreter | Custom Content Sources

For User Guide, press F1

AccessData FTK Imager 4.7.1.2

File View Mode Help

Properties

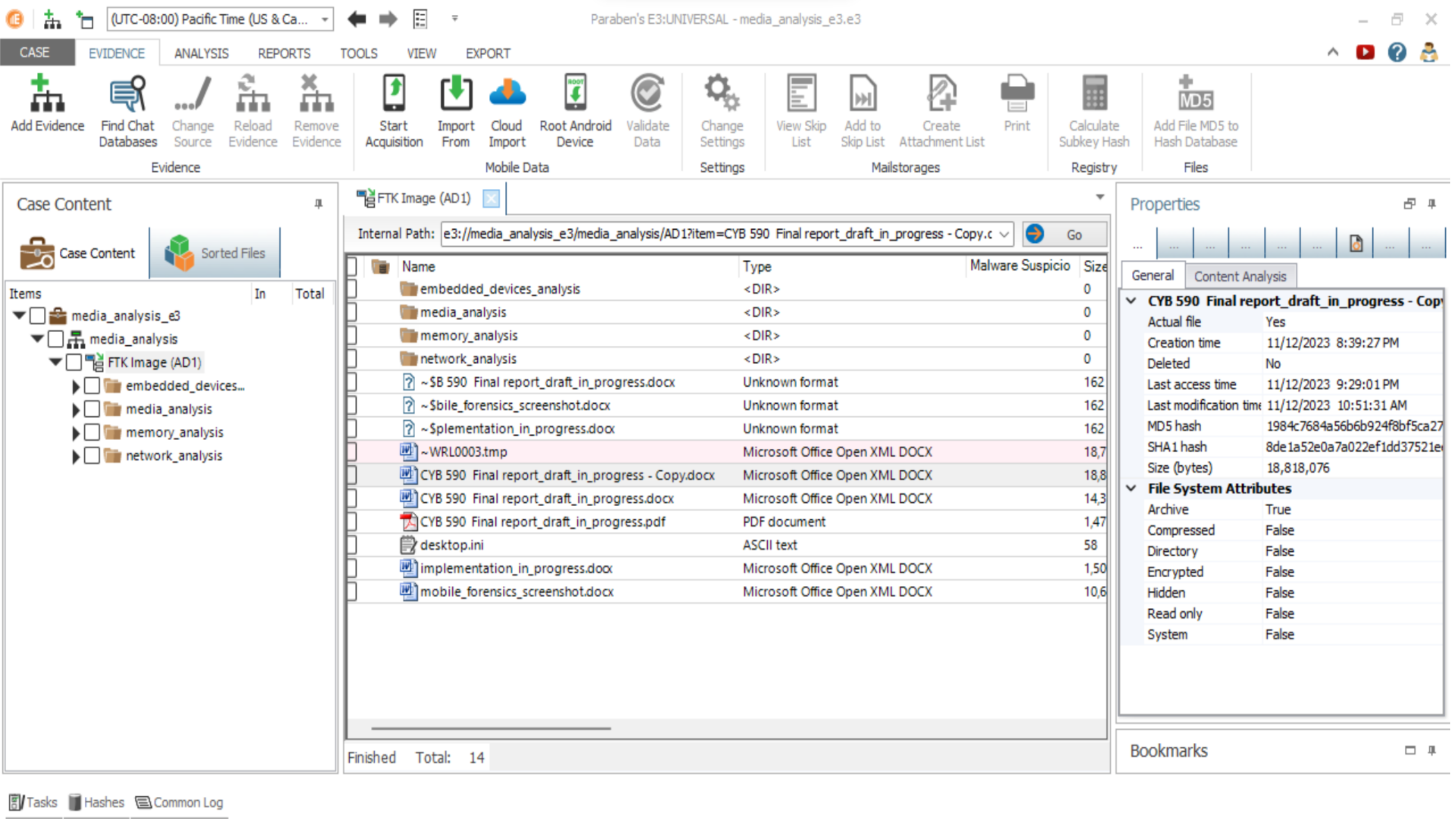
Drive/Image Verify Results

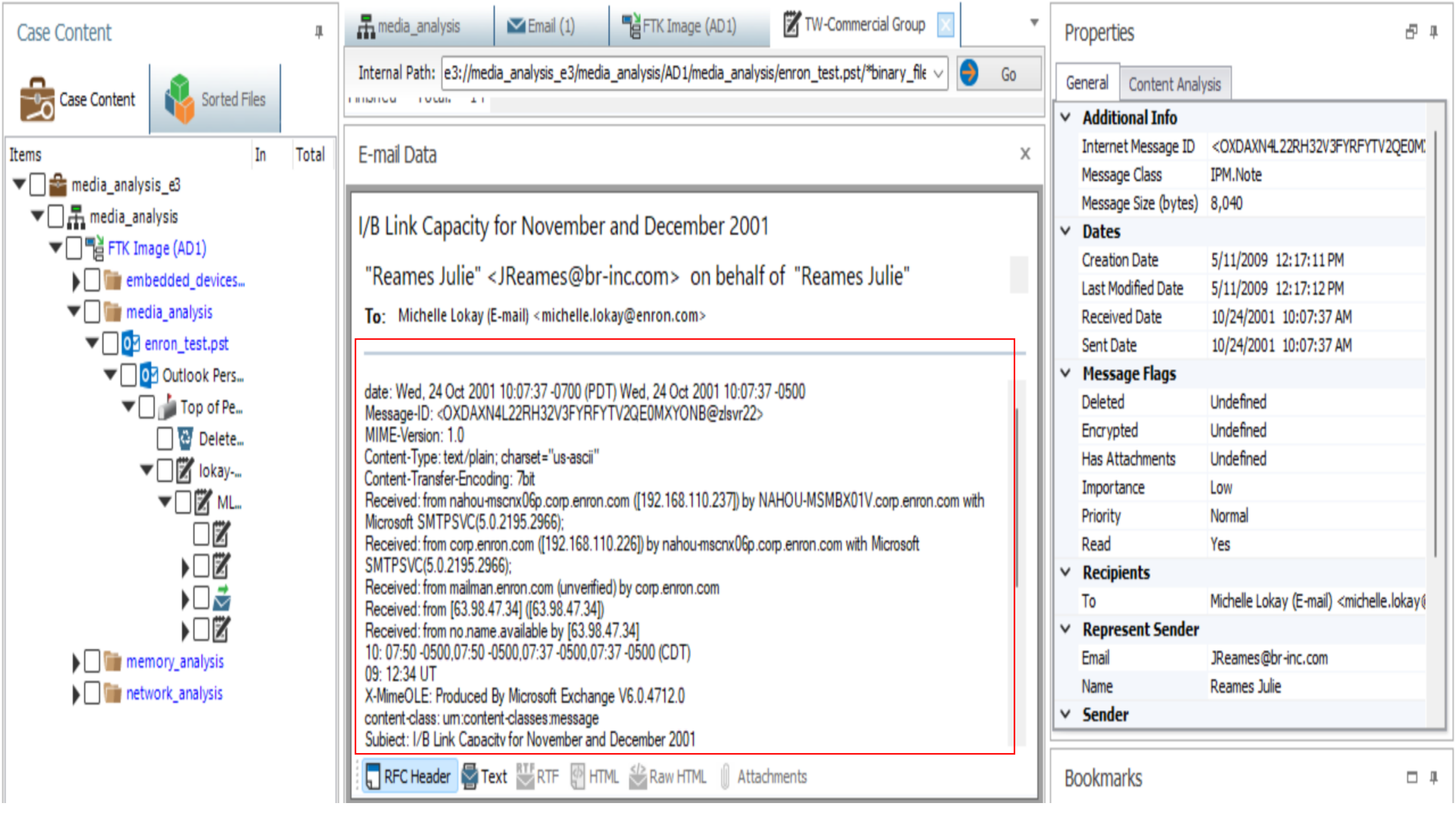
Name	media_analysis.ad1
MD5 Hash	
Computed hash	95f7b39f5cf389ad5e947527bf9df4e9
Report Hash	95f7b39f5cf389ad5e947527bf9df4e9
Verify result	Match
SHA1 Hash	
Computed hash	a107c9779e4f8c9b8d82abe95fd0c3cab61f1938
Report Hash	a107c9779e4f8c9b8d82abe95fd0c3cab61f1938
Verify result	Match

Close

Properties | Hex Value Interpreter | Custom Content Sources

For User Guide, press F1


(UTC-08:00) Pacific Time (US & Ca...
Paraben's E3:UNIVERSAL - media_analysis_e3.e3
CASE
EVIDENCE
ANALYSIS
REPORTS
TOOLS
VIEW
EXPORT
Add Evidence
Find Chat Databases
Change Source
Reload Evidence
Remove Evidence
Evidence
Start Acquisition
Import From
Cloud Import
Root Android Device
Validate Data
Mobile Data
Change Settings
Settings
View Skip List
Add to Skip List
Create Attachment List
Print
Mailstorages
Calculate Subkey Hash
Registry
Add File MD5 to Hash Database
Files
Case Content
Case Content
Sorted Files
Items
In
Total
media_analysis_e3
media_analysis
FTK Image (AD1)
embedded_devices...
media_analysis
memory_analysis
network_analysis
FTK Image (AD1)
Internal Path:
e3://media_analysis_e3/media_analysis/AD1?item=CYB 590 Final report_draft_in_progress - Copy.c
Go
Name
Type
Malware Suspicio
Size
embedded_devices_analysis
<DIR>
0
media_analysis
<DIR>
0
memory_analysis
<DIR>
0
network_analysis
<DIR>
0
~$B 590 Final report_draft_in_progress.docx
Unknown format
162
~$bile_forensics_screenshot.docx
Unknown format
162
~$plementation_in_progress.docx
Unknown format
162
~WRL0003.tmp
Microsoft Office Open XML DOCX
18,7
CYB 590 Final report_draft_in_progress - Copy.docx
Microsoft Office Open XML DOCX
18,8
CYB 590 Final report_draft_in_progress.docx
Microsoft Office Open XML DOCX
14,3
CYB 590 Final report_draft_in_progress.pdf
PDF document
1,47
desktop.ini
ASCII text
58
implementation_in_progress.docx
Microsoft Office Open XML DOCX
1,50
mobile_forensics_screenshot.docx
Microsoft Office Open XML DOCX
10,6
Finished
Total: 14
Properties
General
Content Analysis
CYB 590 Final report_draft_in_progress - Cop
Actual file
Yes
Creation time
11/12/2023 8:39:27 PM
Deleted
No
Last access time
11/12/2023 9:29:01 PM
Last modification time
11/12/2023 10:51:31 AM
MD5 hash
1984c7684a56b6b924f8bf5ca27
SHA1 hash
8de1a52e0a7a022ef1dd37521e
Size (bytes)
18,818,076
File System Attributes
Archive
True
Compressed
False
Directory
False
Encrypted
False
Hidden
False
Read only
False
System
False
Bookmarks
Tasks
Hashes
Common Log


Case Content
Case Content
Sorted Files
Items
In
Total
media_analysis_e3
media_analysis
FTK Image (AD1)
embedded_devices...
media_analysis
enron_test.pst
Outlook Pers...
Top of Pe...
Delete...
lokay-...
ML...
memory_analysis
network_analysis
media_analysis
Email (1)
FTK Image (AD1)
TW-Commercial Group
Internal Path: e3://media_analysis_e3/media_analysis/AD1/media_analysis/enron_test.pst/*binary_file
Go
E-mail Data
I/B Link Capacity for November and December 2001
"Reames Julie" <JReames@br-inc.com> on behalf of "Reames Julie"
To: Michelle Lokay (E-mail) <michelle.lokay@enron.com>
date: Wed, 24 Oct 2001 10:07:37 -0700 (PDT) Wed, 24 Oct 2001 10:07:37 -0500
Message-ID: <OXDAXN4L22RH32V3FYRFYTV2QE0MXYONB@zlsvr22>
MIME-Version: 1.0
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: 7bit
Received: from nahou-mscnx06p.corp.enron.com ([192.168.110.237]) by NAHOU-MSMBX01V.corp.enron.com with Microsoft SMTPSVC(5.0.2195.2966);
Received: from corp.enron.com ([192.168.110.226]) by nahou-mscnx06p.corp.enron.com with Microsoft SMTPSVC(5.0.2195.2966);
Received: from mailman.enron.com (unverified) by corp.enron.com
Received: from [63.98.47.34] ([63.98.47.34])
Received: from no.name.available by [63.98.47.34]
10: 07:50 -0500,07:50 -0500,07:37 -0500,07:37 -0500 (CDT)
09: 12:34 UT
X-MimeOLE: Produced By Microsoft Exchange V6.0.4712.0
content-class: urn:content-classes:message
Subject: I/B Link Capacity for November and December 2001
RFC Header
Text
RTF
HTML
Raw HTML
Attachments
Properties
General
Content Analysis
Additional Info
Internet Message ID
<OXDAXN4L22RH32V3FYRFYTV2QE0M
Message Class
IPM.Note
Message Size (bytes)
8,040
Dates
Creation Date
5/11/2009 12:17:11 PM
Last Modified Date
5/11/2009 12:17:12 PM
Received Date
10/24/2001 10:07:37 AM
Sent Date
10/24/2001 10:07:37 AM
Message Flags
Deleted
Undefined
Encrypted
Undefined
Has Attachments
Undefined
Importance
Low
Priority
Normal
Read
Yes
Recipients
To
Michelle Lokay (E-mail) <michelle.lokay
Represent Sender
Email
JReames@br-inc.com
Name
Reames Julie
Sender
Bookmarks

Generate Report

Reports

Case Content

Case Content | Sorted Files

Items | In | Total

- media_analysis_e3
  - media_analysis
    - FTK Image (AD1)
      - embedded_devices...
      - media_analysis
        - enron_test.pst
          - Outlook Pers...
            - Top of Pe...
              - Delete...
              - lokay-...
                - ML...
      - memory_analysis
      - network_analysis

Reports Wizard

General options

Select General options: report type, destination folder etc. Follow the wizard steps to define what information will be added to the report.

General options

Investigator's Information

Filesystem types

- File properties

Sorted files

Custom Report View

Summary and Conclusion

Logs & Supplementary files

Select the report type to be generated :

(•) HTML Investigative Report	(example)	(all evidence)
( ) Simple Text Report	(example)	(all evidence)
( ) Simple RTF Report	(example)	(all evidence)
( ) CSV Text Report	(example)	(all evidence)
( ) HTML Evidence Summary Report	(example)	(all evidence)
( ) HTML E-mail Message Report	(example)	(e-mail databases only)
( ) E-mail Data Review Report	(example)	(e-mail databases only)
( ) Malware Scan Results Report	(example)	(malware scan results)
( ) Mobile Evidence Timeline Report	(example)	(mobile cases only)
( ) Mobile Evidence PDF Report	(example)	(mobile cases only)
( ) Mobile Excel Spreadsheet Report	(example)	(mobile cases only)
( ) Mobile Data Review Report	(example)	(data included in report)

[ ] Include parsed embedded data

Destination folder :

C:\Users\ysayeed1\Documents\E3 Cases\Reports\ Browse...

[x] Open report on finish [ ] Save current wizard options as default

< Previous | Next > | Finish | Cancel

(UTC-08:00) Pacific Time (US & Ca...

Paraben's E3:UNIVERSAL - android_device.e3

CASE | EVIDENCE | ANALYSIS | REPORTS | TOOLS | VIEW | EXPORT

Add Evidence | Find Chat Databases | Change Source | Reload Evidenc

Evidence

File MD5 to Database

Files

Case Content

Case Content | Sorted Files

Items

android_device

Finished Total: 0

Bookmarks

Tasks | Hashes | Common Log

Acquisition Wizard

Welcome to Acquisition Wizard

Select a device for acquisition:

It might take up to several seconds for a device to be detected after connection to the computer.

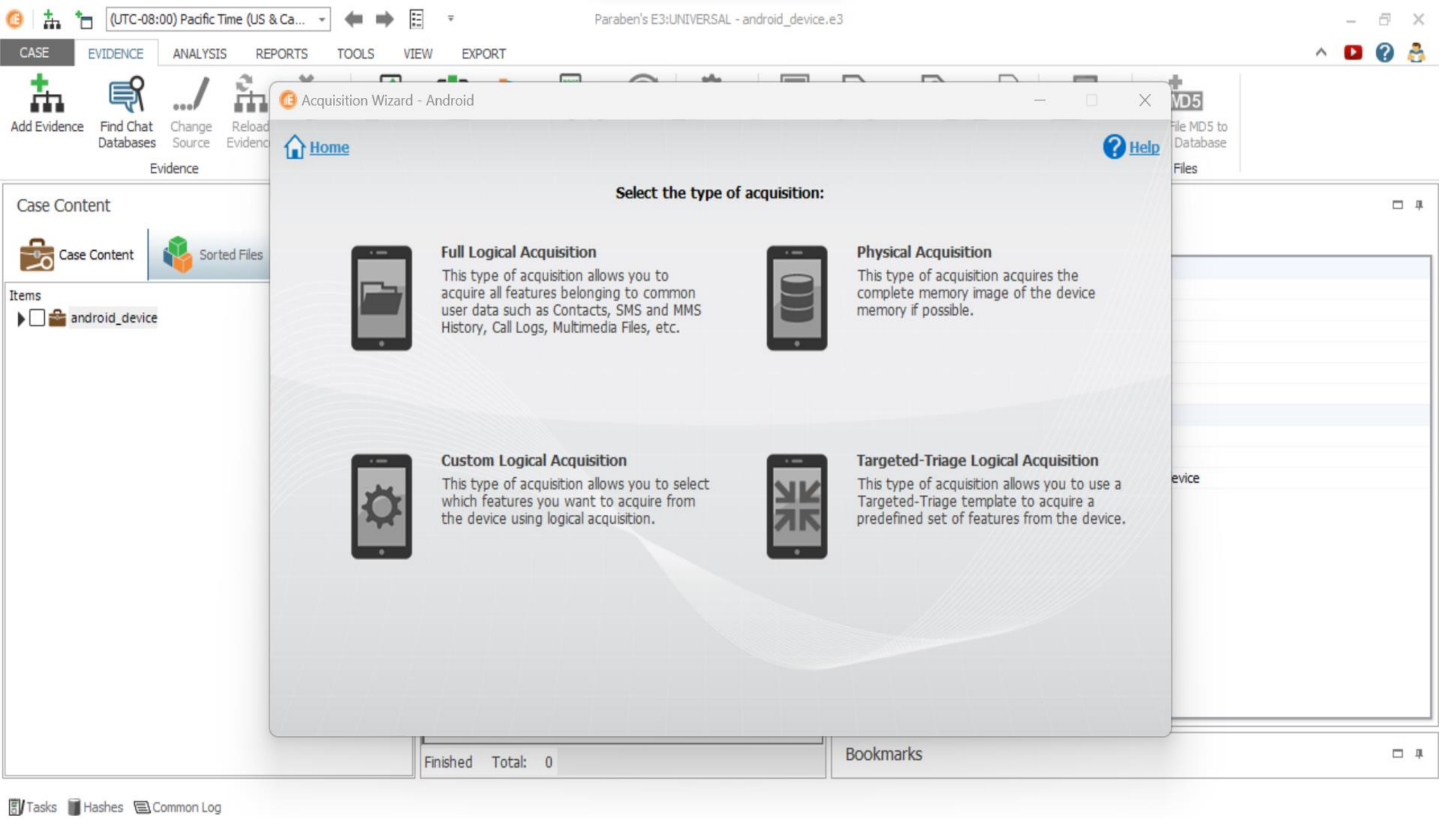
Portable Device

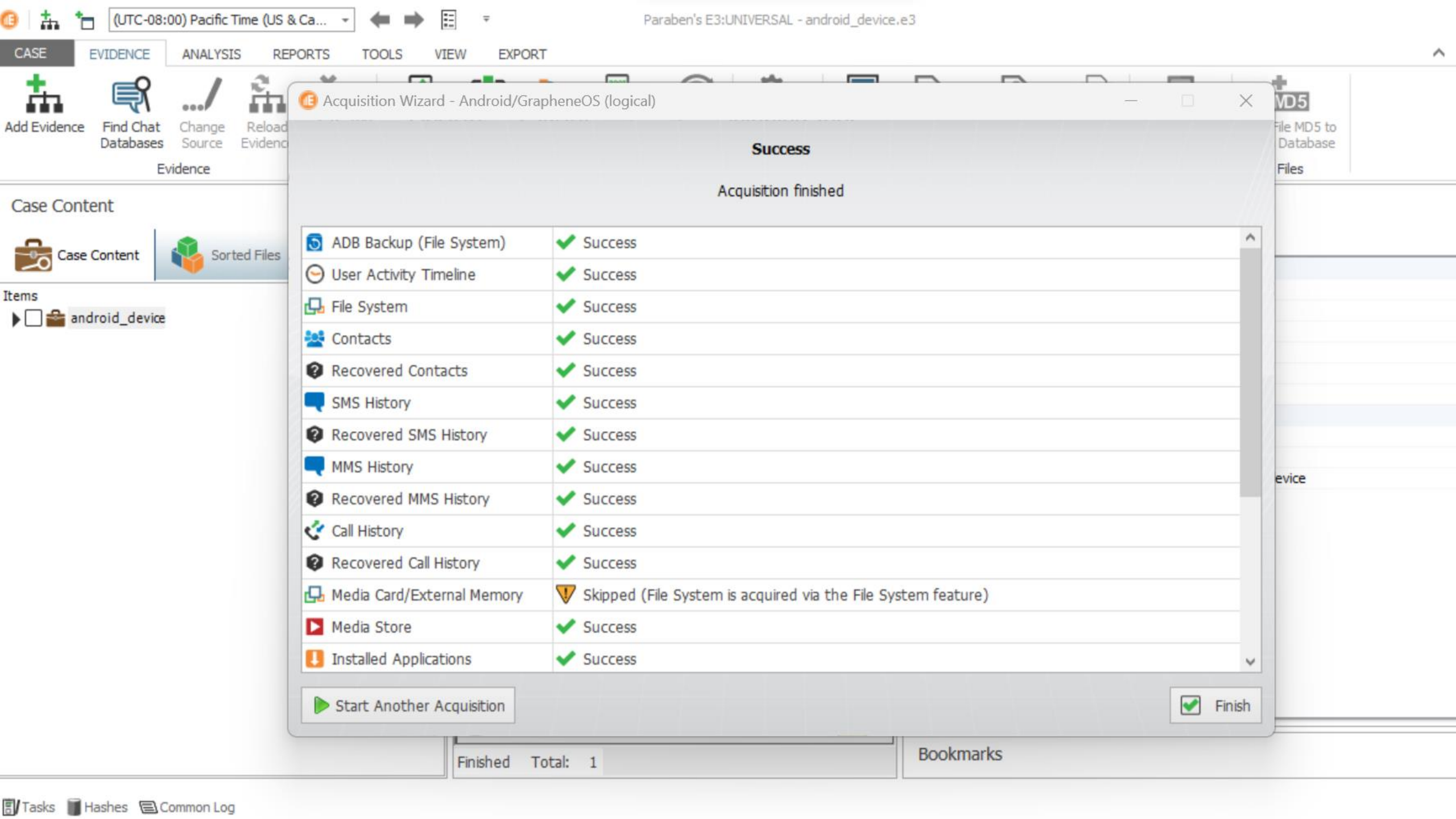
Android

Samsung GSM

Manual plug-in selection

Click here to view troubleshooting instructions if a device is not detected


(UTC-08:00) Pacific Time (US & Ca...
Paraben's E3:UNIVERSAL - android_device.e3
CASE
EVIDENCE
ANALYSIS
REPORTS
TOOLS
VIEW
EXPORT
Add Evidence
Find Chat Databases
Change Source
Reload Evidenc
Evidence
File MD5 to Database
Files
Case Content
Case Content
Sorted Files
Items
android_device
Acquisition Wizard - Android
Home
Help
Select the type of acquisition:
Full Logical Acquisition
This type of acquisition allows you to acquire all features belonging to common user data such as Contacts, SMS and MMS History, Call Logs, Multimedia Files, etc.
Physical Acquisition
This type of acquisition acquires the complete memory image of the device memory if possible.
Custom Logical Acquisition
This type of acquisition allows you to select which features you want to acquire from the device using logical acquisition.
Targeted-Triage Logical Acquisition
This type of acquisition allows you to use a Targeted-Triage template to acquire a predefined set of features from the device.
Finished
Total: 0
Bookmarks
Tasks
Hashes
Common Log


(UTC-08:00) Pacific Time (US & Ca...
Paraben's E3:UNIVERSAL - android_device.e3
CASE
EVIDENCE
ANALYSIS
REPORTS
TOOLS
VIEW
EXPORT
Add Evidence
Find Chat Databases
Change Source
Reload Evidenc
Evidence
File MD5 to Database
Files
Case Content
Case Content
Sorted Files
Items
android_device
Acquisition Wizard - Android/GrapheneOS (logical)
Success
Acquisition finished
ADB Backup (File System) Success
User Activity Timeline Success
File System Success
Contacts Success
Recovered Contacts Success
SMS History Success
Recovered SMS History Success
MMS History Success
Recovered MMS History Success
Call History Success
Recovered Call History Success
Media Card/External Memory Skipped (File System is acquired via the File System feature)
Media Store Success
Installed Applications Success
Start Another Acquisition
Finish
Finished Total: 1
Bookmarks
Tasks
Hashes
Common Log

(UTC-08:00) Pacific Time (US & Ca...

Paraben's E3:UNIVERSAL - android_device.e3

CASE | EVIDENCE | ANALYSIS | REPORTS | TOOLS | VIEW | EXPORT

Add Evidence | Find Chat Databases | Change Source | Reload Evidence | Remove Evidence — Evidence

Start Acquisition | Import From | Cloud Import | Root Android Device | Validate Data — Mobile Data

Change Settings — Settings

View Skip List | Add to Skip List | Create Attachment List | Print — Mailstorages

Calculate Subkey Hash — Registry

Add File MD5 to Hash Database — Files

Case Content

Case Content | Sorted Files

Items

- Contacts
- SMS
- MMS
- Call History
  - Call History
- Media Store
- Installed Applications
- Default Browser History
- Settings
- Authentication Data
- Calendar
- Attached Files
- Mobile Data Triage
  - Device Information
  - Installed Applications
  - Contact Email Accounts
  - ICE Contacts
  - Locations
  - Recent Web Searches

Device Information

Internal Path: e3://android_device/android_device_Acquisition_11-08-2023_10-55-48/E3 data case/Mobile Data Tr | Go

Name	Value
Program timestam	11/8/2023 10:56:38 AM
Acquisition Type	Android/GrapheneOS Logica
Serial Number(RO)	5200fd0d4e2c661f
Serial Number(RIL)	R58M721H2ZZ
SIM Serial	89148000005034700716
Device ID (IMEI)	357092102515786
Subscriber ID (IMSI	311480496736261
Device Software Ve	01
Line 1 Number	3104152051
Network Operator	310000
Network Operator	Searching for Service
Network Type	Unknown
Phone Type	CDMA
SIM Operator	311480
SIM Operator Nam	Verizon
SIM is present (Slot	Yes
SIM is present (Slot	Unknown
Board	universal7885
Brand	samsung
Device	j7topeltetfnvzw

Finished Total: 30

Properties

General | Content Anal

Common

Extracting Text	N/A
Keywords Inde	N/A
Malware Scan (	N/A
Sorting	N/A

Bookmarks

Tasks | Hashes | Common Log

(UTC-08:00) Pacific Time (US & Ca...

Paraben's E3:UNIVERSAL - android_device.e3

CASE | EVIDENCE | ANALYSIS | REPORTS | TOOLS | VIEW | EXPORT

Add Evidence | Find Chat Databases | Change Source | Reload Evidence | Remove Evidence — Evidence

Start Acquisition | Import From | Cloud Import | Root Android Device | Validate Data — Mobile Data

Change Settings — Settings

View Skip List | Add to Skip List | Create Attachment List | Print — Mailstorages

Calculate Subkey Hash — Registry

Add File MD5 to Hash Database — Files

Case Content

Case Content | Sorted Files

Items

- Contacts
- SMS
- MMS
- Call History
  - Call History
- Media Store
- Installed Applications
- Default Browser History
- Settings
- Authentication Data
- Calendar
- Attached Files
- Mobile Data Triage
  - Device Information
  - Installed Applications
  - Contact Email Accounts
  - ICE Contacts
  - Locations
  - Recent Web Searches

Installed Applicatio...

Internal Path: e3://android_device/android_device_Acquisition_11-08-2023_10-55-48/E3 data case/Mobile Data Tr | Go

Icon	Application Name	Version	Internal Application N
	1Weather	5.3.7.2	com.handmark.expre
	Android Accessibility Suite	13.1.0.501229322	com.google.android.
	ANT Radio Service	4.16.00	com.dsi.ant.service.sc
	ANT+ Plugins Service	3.6.40	com.dsi.ant.plugins.a
	Briefing	3.4.2	flipboard.boxer.app
	Calculator	6.0.60.20	com.sec.android.app.
	Chrome	80.0.3987.132	com.android.chrome
	ConfigAPK	1001	android.autoinstalls.c
	Device maintenance	2.0.31.1	com.samsung.androi
	Drive	2.18.432.04.34	com.google.android.
	Duo	43.0.222101433.DR43_RC20	com.google.android.
	Email	6.1.75.0	com.samsung.androi
	Facebook	405.0.0.23.72	com.facebook.katana
	Forensic Connector	1.10.7-29194(F)	com.compelson.mefc
	Gmail	2023.02.05.512982913.Release	com.google.android.
	Google	14.9.9.26.arm	com.google.android.ox
	Google Play Movies & TV	4.8.20.18	com.google.android.
	Google Play Music	8.16.7620-1J	com.google.android.

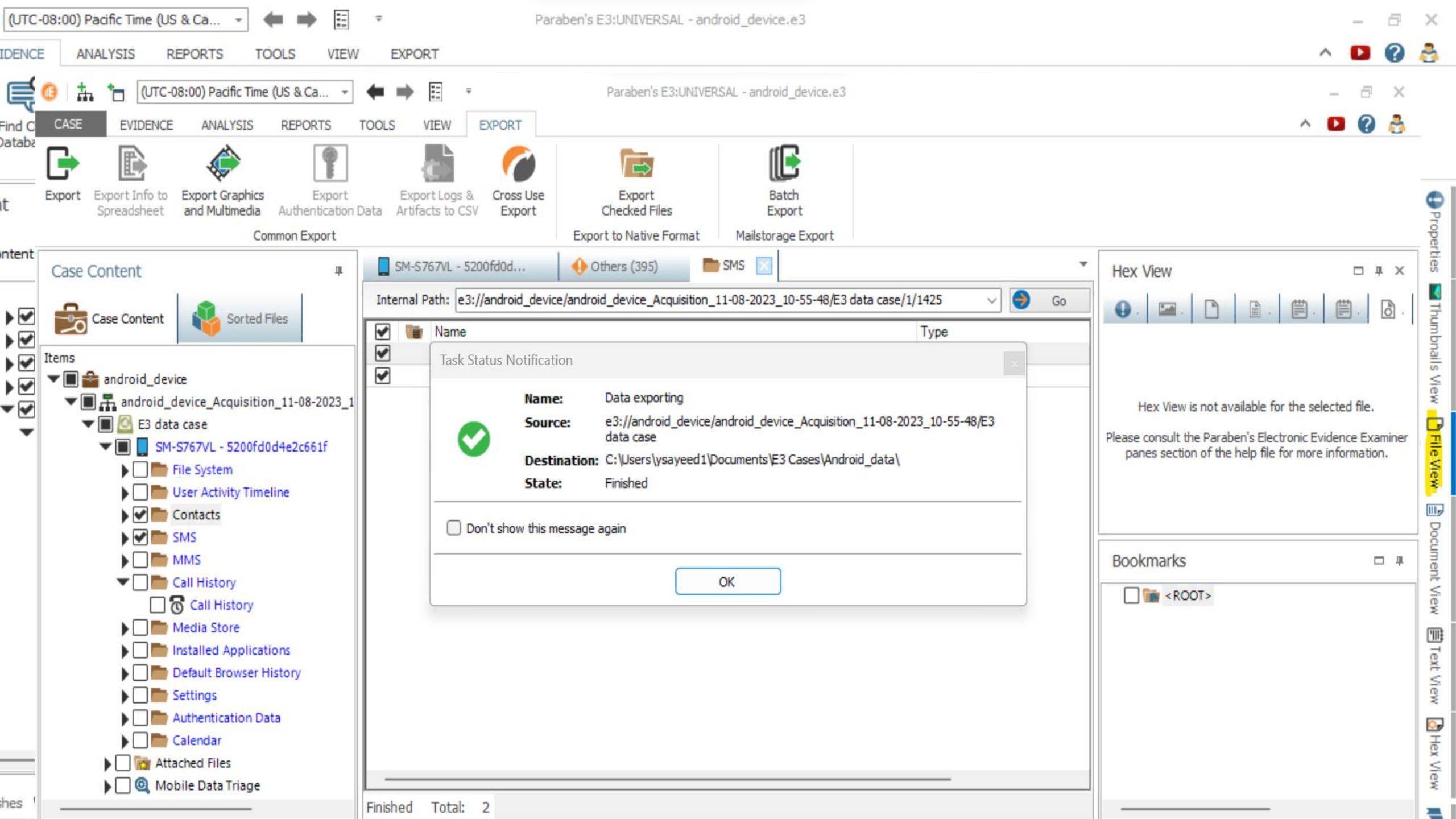
Finished Total: 32

Properties

General | Content Analysis

Common	
Extracting Text	N/A
Keywords Inde	N/A
Malware Scan (	N/A
Sorting	N/A

Bookmarks


(UTC-08:00) Pacific Time (US & Ca...
Paraben's E3:UNIVERSAL - android_device.e3
IDENCE
ANALYSIS
REPORTS
TOOLS
VIEW
EXPORT
(UTC-08:00) Pacific Time (US & Ca...
Paraben's E3:UNIVERSAL - android_device.e3
CASE
EVIDENCE
ANALYSIS
REPORTS
TOOLS
VIEW
EXPORT
Export
Export Info to Spreadsheet
Export Graphics and Multimedia
Export Authentication Data
Export Logs & Artifacts to CSV
Cross Use Export
Common Export
Export Checked Files
Export to Native Format
Batch Export
Mailstorage Export
Case Content
Case Content
Sorted Files
Items
android_device
android_device_Acquisition_11-08-2023_1
E3 data case
SM-S767VL - 5200fd0d4e2c661f
File System
User Activity Timeline
Contacts
SMS
MMS
Call History
Call History
Media Store
Installed Applications
Default Browser History
Settings
Authentication Data
Calendar
Attached Files
Mobile Data Triage
SM-S767VL - 5200fd0d...
Others (395)
SMS
Internal Path:
e3://android_device/android_device_Acquisition_11-08-2023_10-55-48/E3 data case/1/1425
Go
Name
Type
Task Status Notification
Name: Data exporting
Source: e3://android_device/android_device_Acquisition_11-08-2023_10-55-48/E3 data case
Destination: C:\Users\ysayeed1\Documents\E3 Cases\Android_data\
State: Finished
Don't show this message again
OK
Finished
Total: 2
Hex View
Hex View is not available for the selected file.
Please consult the Paraben's Electronic Evidence Examiner panes section of the help file for more information.
Bookmarks
<ROOT>
Properties
Thumbnails View
File View
Document View
Text View
Hex View

Conclusion & Future Work

- By implementing digital forensics incidence response, teams can address lack of skills and mismanagement with “Centralized” and “Distributed” model.
- Proper “intelligence” in the threat intelligence is provided to incident responders by using Digital Forensics Incident response tools which are adequate, managed, tested, and efficiently utilized.
- Improved resiliency against future attacks.
- Gather evidence you need to press charge against the criminals.
- DFIR provides a structured and systematic approach to handling security incidents.
- Applying machine learning methods to automate network analysis section wherein all the logs and packet captures should be periodically cleaned and transformed into data frames. From these data frames, AI algorithms can be used to plot the analysis in the form of data visualization to detect the alert swiftly in an optimized manner.

References

[1] Ben Filipkowski. (2023, April 20). Digital Forensics and Incident Response. https://fieldeffect.com/blog/digital-forensics-incident-response

[2] Sara Jelen. (2023, June 29). Incident Response in Cybersecurity: Preparing for a Security Breach. https://securitytrails.com/blog/incident-response

[3] Fazila Malik. (2023, July 31). Writing Your Security Incident Response Policy. https://www.strongdm.com/blog/writing-your-security-incident-response-policy

[4] Chapple, M., Stewart, J. M., & Gibson, D. (2021). (ISC)² CISSP Certified Information Systems Security Professional Official Study Guide (9th ed.).

[5] Cynet. (n.d.). NIST Cybersecurity Framework: A Comprehensive Guide. Cynet. https://www.cynet.com/nist- cybersecurity-framework/

[6] NetWitness Investigator, https://www.netwitness.com/

[7] Wireshark, https://www.wireshark.org/

[8] Access data Forensic Tool Kit, https://www.exterro.com/forensic-toolkit

[9] Paraben's Electronic Evidene Examiner (E3), https://paraben.com/

Any Queries

Thank You