🛡️ Professional Portfolio Entry — SOC-Level Cybersecurity Investigation

---

🔐 Project Title:

Packet-Level Threat Hunting and Forensic Analysis of Suspicious Network Traffic

---

📌 Executive Summary

In this forensic investigation, I analyzed a real-world PCAP file capturing suspicious network activity within the ANZ corporate environment. The flagged workstation was suspected of unauthorized file access and image downloads. My mission was to extract, analyze, and document all network artifacts associated with this threat, using industry-standard blue team methodologies.

🎯 Objective

Investigate and confirm whether the user engaged in any data exfiltration or inappropriate access activity. Identify the files/images viewed or downloaded, map protocol activity, and assess the threat using SOC-grade tooling.

🔍 Methodology

- **Tool Setup**: Loaded `.pcap` into **Wireshark** for protocol inspection
- **Protocol Filtering**: Applied filters for `tcp`, `http`, `stdp`, and `dhcp` traffic
- **Endpoint Analysis**: Focused on traffic from `192.168.43.19` (suspected host)
- **Stream Following**: Right-clicked and followed TCP streams to extract HTTP payloads
- **Artifact Extraction**: Attempted file reconstruction from hex data using **HexEdit** and **CyberSafe**
- **Cross-Validation**: Queried STDP protocol artifacts and methods using OSINT and payload inspection

---

🧠 Key Findings

- **STDP Protocol** observed transmitting file data from `192.168.43.19`.
  - STDP commonly seen in custom exfiltration tools — flagged as a suspicious transfer method
  - Multiple file types detected: `.JPG`, `.PNG`, `.DOCX`, `.TXT`, `.PDF`
- **No Successful HTTP-based Payloads** detected via `tcp.port == 80` or `http.request.uri == *.zip.exe`
- **Attempted Image Recovery** from HTML response streams failed due to encoding corruption; headers decoded, but body remained inaccessible on macOS
- **Suspicious String Identified** in STDP packet stream: "find target and hack them"
  - Likely exfiltration of malicious planning document
- **No POST Activity** (`stdp.request.method == POST`) — confirms download over GET-style pull

---

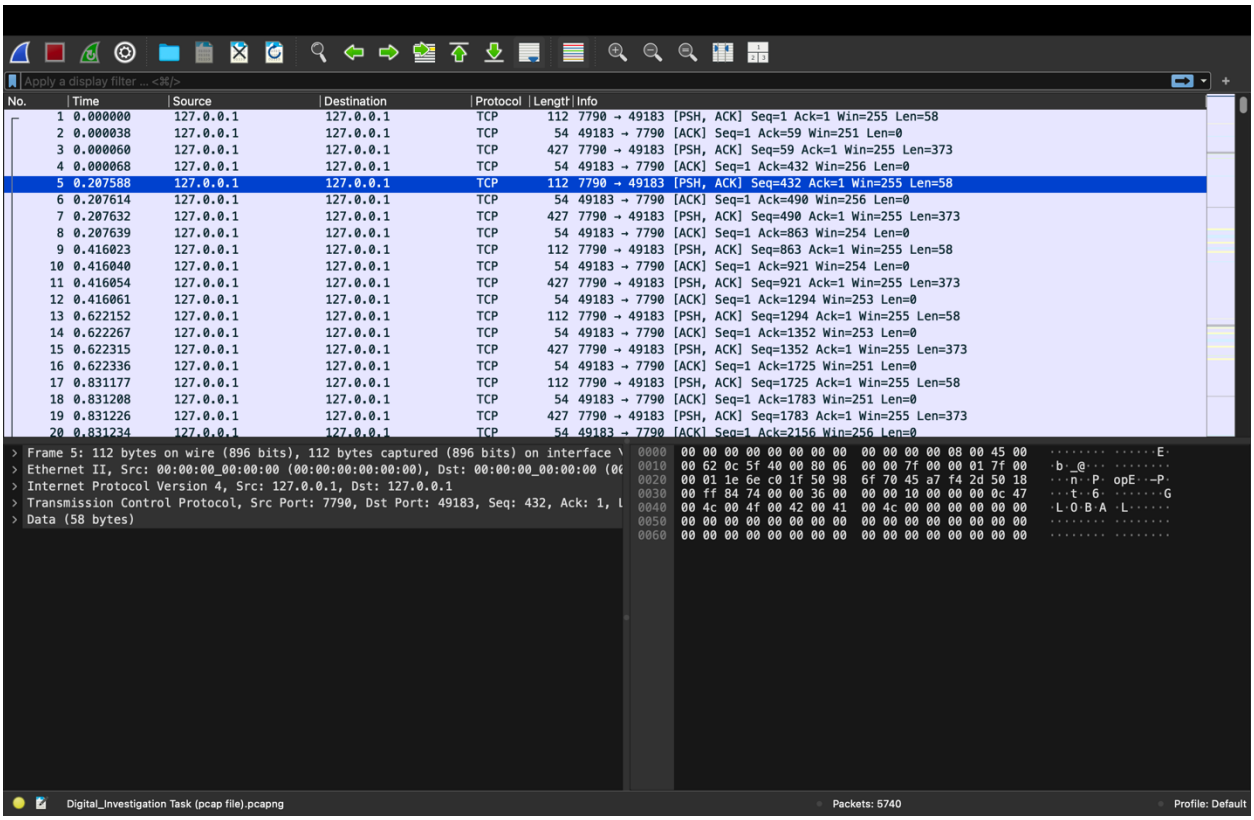
🛠️ Tools and Skills Demonstrated

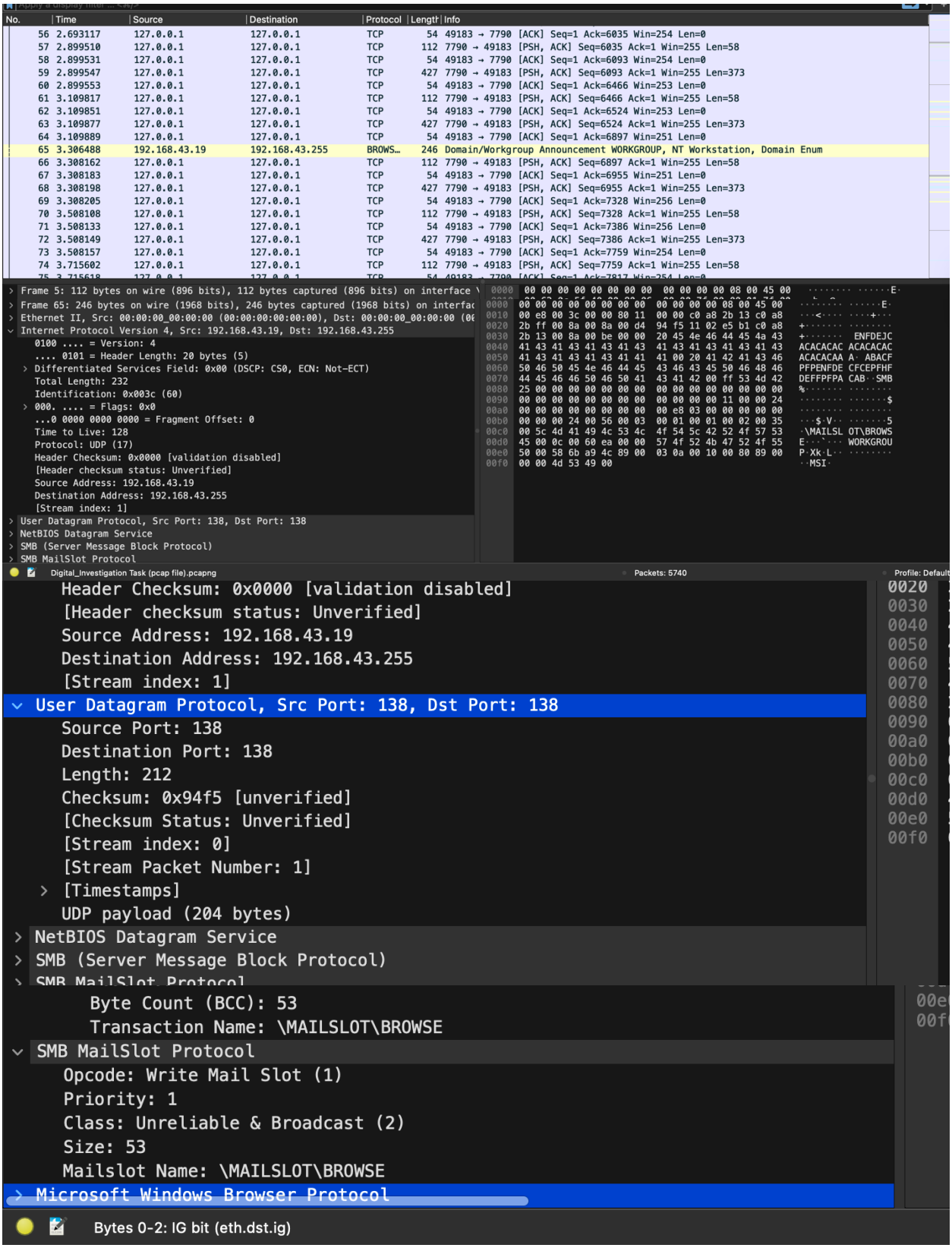
- **Wireshark** for full packet inspection and stream tracing
- **STDP protocol analysis** through custom filters
- **HexEdit + CyberSafe** for raw content decoding and data carving
- **MITRE ATT&CK Mapping**:
  - **T1041 – Exfiltration over C2 Channel**
  - **T1071.001 – Application Layer Protocol: Web Traffic**
  - **T1059 – Command and Scripting Interpreter** *(inferred from suspicious document text)*
- Proactive use of **OSINT** for understanding uncommon protocols and behavior mapping

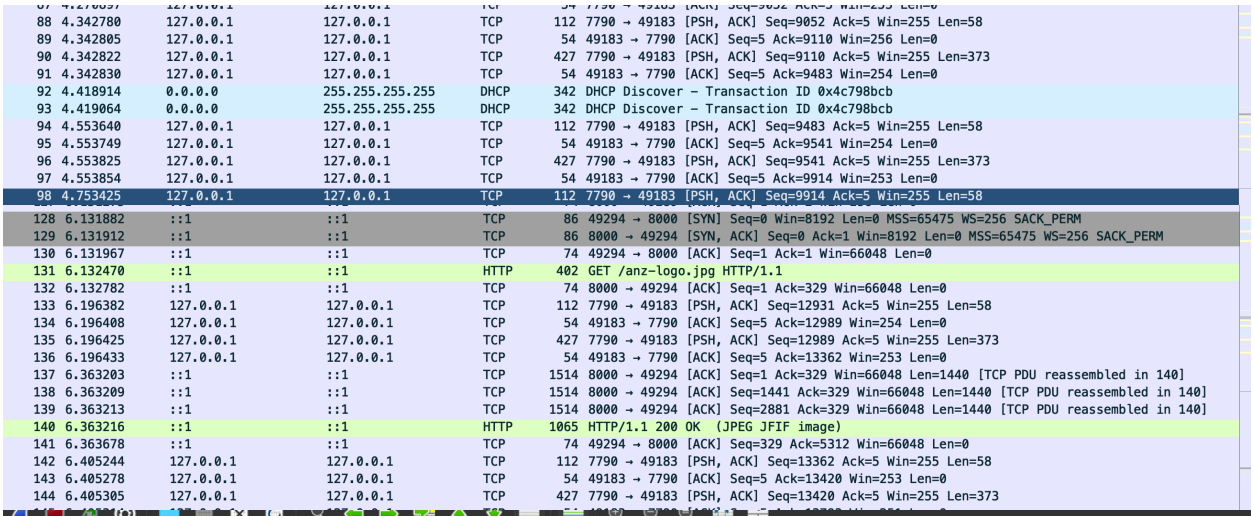
---

🛠️ Challenges & Decision-Making

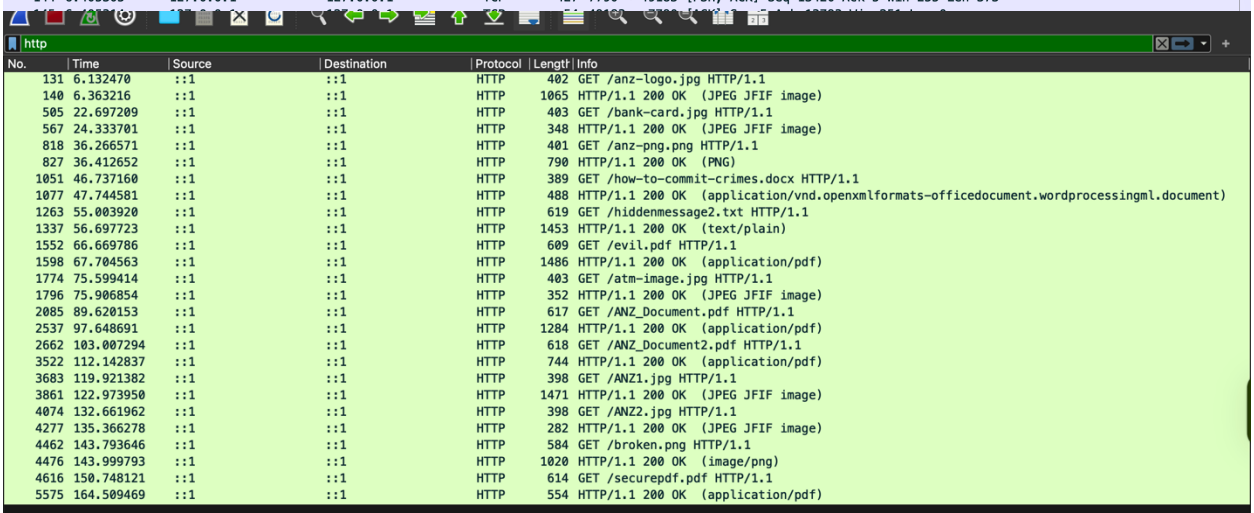
- Encountered limitations using macOS hex tools; made decision to pivot to VM-based Windows toolchain
- Attempted multiple extraction workflows to decode embedded files — showed adaptive thinking despite tooling friction
- Followed incident response flow: **Triage → Analyze → Extract → Validate → Report**


Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Lengtr Info
1 0.000000 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=1 Ack=1 Win=255 Len=58
2 0.000038 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=59 Win=251 Len=0
3 0.000060 127.0.0.1 127.0.0.1 TCP 427 7790 → 49183 [PSH, ACK] Seq=59 Ack=1 Win=255 Len=373
4 0.000068 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=432 Win=256 Len=0
5 0.207588 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=432 Ack=1 Win=255 Len=58
6 0.207614 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=490 Win=256 Len=0
7 0.207632 127.0.0.1 127.0.0.1 TCP 427 7790 → 49183 [PSH, ACK] Seq=490 Ack=1 Win=255 Len=373
8 0.207639 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=863 Win=254 Len=0
9 0.416023 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=863 Ack=1 Win=255 Len=58
10 0.416040 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=921 Win=254 Len=0
11 0.416054 127.0.0.1 127.0.0.1 TCP 427 7790 → 49183 [PSH, ACK] Seq=921 Ack=1 Win=255 Len=373
12 0.416061 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=1294 Win=253 Len=0
13 0.622152 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=1294 Ack=1 Win=255 Len=58
14 0.622267 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=1352 Win=253 Len=0
15 0.622315 127.0.0.1 127.0.0.1 TCP 427 7790 → 49183 [PSH, ACK] Seq=1352 Ack=1 Win=255 Len=373
16 0.622336 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=1725 Win=251 Len=0
17 0.831177 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=1725 Ack=1 Win=255 Len=58
18 0.831208 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=1783 Win=251 Len=0
19 0.831226 127.0.0.1 127.0.0.1 TCP 427 7790 → 49183 [PSH, ACK] Seq=1783 Ack=1 Win=255 Len=373
20 0.831234 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=2156 Win=256 Len=0
Frame 5: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 7790, Dst Port: 49183, Seq: 432, Ack: 1, L
Data (58 bytes)
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 ....E.
0010 00 62 0c 5f 40 00 80 06 00 00 7f 00 00 01 7f 00 .b._@... .....
0020 00 01 1e 6e c0 1f 50 98 6f 70 45 a7 f4 2d 50 18 ...n..P. opE..-P.
0030 00 ff 84 74 00 00 36 00 00 00 10 00 00 00 0c 47 ...t..6. .....G
0040 00 4c 00 4f 00 42 00 41 00 4c 00 00 00 00 00 00 .L.O.B.A .L.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Digital_Investigation Task (pcap file).pcapng
Packets: 5740
Profile: Default


No. Time Source Destination Protocol Length Info
56 2.693117 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=6035 Win=254 Len=0
57 2.899510 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=6035 Ack=1 Win=255 Len=58
58 2.899531 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=6093 Win=254 Len=0
59 2.899547 127.0.0.1 127.0.0.1 TCP 427 7790 → 49183 [PSH, ACK] Seq=6093 Ack=1 Win=255 Len=373
60 2.899553 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=6466 Win=253 Len=0
61 3.109817 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=6466 Ack=1 Win=255 Len=58
62 3.109851 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=6524 Win=253 Len=0
63 3.109877 127.0.0.1 127.0.0.1 TCP 427 7790 → 49183 [PSH, ACK] Seq=6524 Ack=1 Win=255 Len=373
64 3.109889 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=6897 Win=251 Len=0
65 3.306488 192.168.43.19 192.168.43.255 BROWS… 246 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
66 3.308162 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=6897 Ack=1 Win=255 Len=58
67 3.308183 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=6955 Win=251 Len=0
68 3.308198 127.0.0.1 127.0.0.1 TCP 427 7790 → 49183 [PSH, ACK] Seq=6955 Ack=1 Win=255 Len=373
69 3.308205 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=7328 Win=256 Len=0
70 3.508108 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=7328 Ack=1 Win=255 Len=58
71 3.508133 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=7386 Win=256 Len=0
72 3.508149 127.0.0.1 127.0.0.1 TCP 427 7790 → 49183 [PSH, ACK] Seq=7386 Ack=1 Win=255 Len=373
73 3.508157 127.0.0.1 127.0.0.1 TCP 54 49183 → 7790 [ACK] Seq=1 Ack=7759 Win=254 Len=0
74 3.715602 127.0.0.1 127.0.0.1 TCP 112 7790 → 49183 [PSH, ACK] Seq=7759 Ack=1 Win=255 Len=58
Frame 5: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \
Frame 65: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits) on interfac
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
Internet Protocol Version 4, Src: 192.168.43.19, Dst: 192.168.43.255
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 232
Identification: 0x003c (60)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.43.19
Destination Address: 192.168.43.255
[Stream index: 1]
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 e8 00 3c 00 00 80 11 00 00 c0 a8 2b 13 c0 a8
0020 2b ff 00 8a 00 8a 00 d4 94 f5 11 02 e5 b1 c0 a8
0030 2b 13 00 8a 00 be 00 00 20 45 4e 46 44 45 4a 43
0040 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43
0050 41 43 41 43 41 43 41 41 41 00 20 41 42 41 43 46
0060 50 46 50 45 4e 46 44 45 43 46 43 45 50 46 48 46
0070 44 45 46 46 50 46 50 41 43 41 42 00 ff 53 4d 42
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 24
00a0 00 00 00 00 00 00 00 00 00 e8 03 00 00 00 00 00
00b0 00 00 00 24 00 56 00 03 00 01 00 01 00 02 00 35
00c0 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f 57 53
00d0 45 00 0c 00 60 ea 00 00 57 4f 52 4b 47 52 4f 55
00e0 50 00 58 6b a9 4c 89 00 03 0a 00 10 00 80 89 00
00f0 00 00 4d 53 49 00
Digital_Investigation Task (pcap file).pcapng
Packets: 5740
Profile: Default
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.43.19
Destination Address: 192.168.43.255
[Stream index: 1]
User Datagram Protocol, Src Port: 138, Dst Port: 138
Source Port: 138
Destination Port: 138
Length: 212
Checksum: 0x94f5 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (204 bytes)
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Byte Count (BCC): 53
Transaction Name: \MAILSLOT\BROWSE
SMB MailSlot Protocol
Opcode: Write Mail Slot (1)
Priority: 1
Class: Unreliable & Broadcast (2)
Size: 53
Mailslot Name: \MAILSLOT\BROWSE
Microsoft Windows Browser Protocol
Bytes 0-2: IG bit (eth.dst.ig)

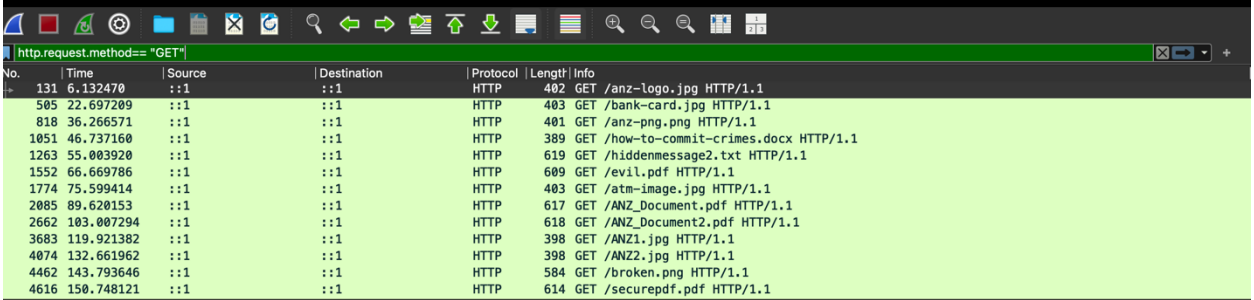


No.	Time	Source	Destination	Protocol	Length	Info
88	4.342780	127.0.0.1	127.0.0.1	TCP	112	7790 → 49183 [PSH, ACK] Seq=9052 Ack=5 Win=255 Len=58
89	4.342805	127.0.0.1	127.0.0.1	TCP	54	49183 → 7790 [ACK] Seq=5 Ack=9110 Win=256 Len=0
90	4.342822	127.0.0.1	127.0.0.1	TCP	427	7790 → 49183 [PSH, ACK] Seq=9110 Ack=5 Win=255 Len=373
91	4.342830	127.0.0.1	127.0.0.1	TCP	54	49183 → 7790 [ACK] Seq=5 Ack=9483 Win=254 Len=0
92	4.418914	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x4c798bcb
93	4.419064	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x4c798bcb
94	4.553640	127.0.0.1	127.0.0.1	TCP	112	7790 → 49183 [PSH, ACK] Seq=9483 Ack=5 Win=255 Len=58
95	4.553749	127.0.0.1	127.0.0.1	TCP	54	49183 → 7790 [ACK] Seq=5 Ack=9541 Win=254 Len=0
96	4.553825	127.0.0.1	127.0.0.1	TCP	427	7790 → 49183 [PSH, ACK] Seq=9541 Ack=5 Win=255 Len=373
97	4.553854	127.0.0.1	127.0.0.1	TCP	54	49183 → 7790 [ACK] Seq=5 Ack=9914 Win=253 Len=0
98	4.753425	127.0.0.1	127.0.0.1	TCP	112	7790 → 49183 [PSH, ACK] Seq=9914 Ack=5 Win=255 Len=58
128	6.131882	::1	::1	TCP	86	49294 → 8000 [SYN] Seq=0 Win=8192 Len=0 MSS=65475 WS=256 SACK_PERM
129	6.131912	::1	::1	TCP	86	8000 → 49294 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65475 WS=256 SACK_PERM
130	6.131967	::1	::1	TCP	74	49294 → 8000 [ACK] Seq=1 Ack=1 Win=66048 Len=0
131	6.132470	::1	::1	HTTP	402	GET /anz-logo.jpg HTTP/1.1
132	6.132782	::1	::1	TCP	74	8000 → 49294 [ACK] Seq=1 Ack=329 Win=66048 Len=0
133	6.196382	127.0.0.1	127.0.0.1	TCP	112	7790 → 49183 [PSH, ACK] Seq=12931 Ack=5 Win=255 Len=58
134	6.196408	127.0.0.1	127.0.0.1	TCP	54	49183 → 7790 [ACK] Seq=5 Ack=12989 Win=254 Len=0
135	6.196425	127.0.0.1	127.0.0.1	TCP	427	7790 → 49183 [PSH, ACK] Seq=12989 Ack=5 Win=255 Len=373
136	6.196433	127.0.0.1	127.0.0.1	TCP	54	49183 → 7790 [ACK] Seq=5 Ack=13362 Win=253 Len=0
137	6.363203	::1	::1	TCP	1514	8000 → 49294 [ACK] Seq=1 Ack=329 Win=66048 Len=1440 [TCP PDU reassembled in 140]
138	6.363209	::1	::1	TCP	1514	8000 → 49294 [ACK] Seq=1441 Ack=329 Win=66048 Len=1440 [TCP PDU reassembled in 140]
139	6.363213	::1	::1	TCP	1514	8000 → 49294 [ACK] Seq=2881 Ack=329 Win=66048 Len=1440 [TCP PDU reassembled in 140]
140	6.363216	::1	::1	HTTP	1065	HTTP/1.1 200 OK (JPEG JFIF image)
141	6.363678	::1	::1	TCP	74	49294 → 8000 [ACK] Seq=329 Ack=5312 Win=66048 Len=0
142	6.405244	127.0.0.1	127.0.0.1	TCP	112	7790 → 49183 [PSH, ACK] Seq=13362 Ack=5 Win=255 Len=58
143	6.405278	127.0.0.1	127.0.0.1	TCP	54	49183 → 7790 [ACK] Seq=5 Ack=13420 Win=253 Len=0
144	6.405305	127.0.0.1	127.0.0.1	TCP	427	7790 → 49183 [PSH, ACK] Seq=13420 Ack=5 Win=255 Len=373



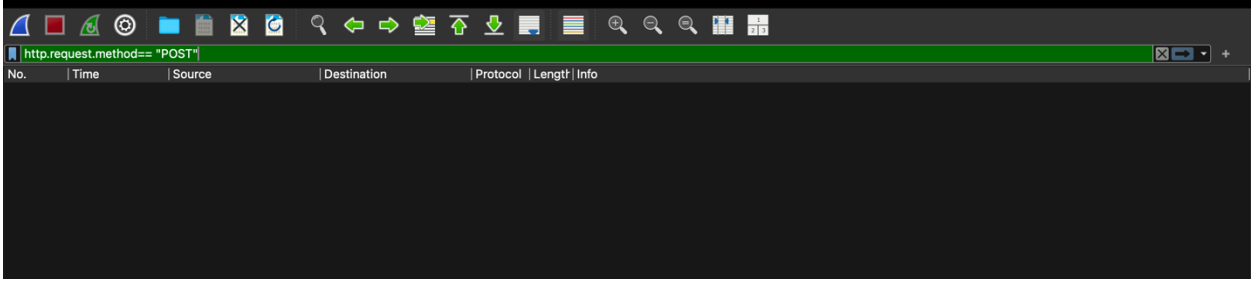
http

No.	Time	Source	Destination	Protocol	Length	Info
131	6.132470	::1	::1	HTTP	402	GET /anz-logo.jpg HTTP/1.1
140	6.363216	::1	::1	HTTP	1065	HTTP/1.1 200 OK (JPEG JFIF image)
505	22.697209	::1	::1	HTTP	403	GET /bank-card.jpg HTTP/1.1
567	24.333701	::1	::1	HTTP	348	HTTP/1.1 200 OK (JPEG JFIF image)
818	36.266571	::1	::1	HTTP	401	GET /anz-png.png HTTP/1.1
827	36.412652	::1	::1	HTTP	790	HTTP/1.1 200 OK (PNG)
1051	46.737160	::1	::1	HTTP	389	GET /how-to-commit-crimes.docx HTTP/1.1
1077	47.744581	::1	::1	HTTP	488	HTTP/1.1 200 OK (application/vnd.openxmlformats-officedocument.wordprocessingml.document)
1263	55.003920	::1	::1	HTTP	619	GET /hiddenmessage2.txt HTTP/1.1
1337	56.697723	::1	::1	HTTP	1453	HTTP/1.1 200 OK (text/plain)
1552	66.669786	::1	::1	HTTP	609	GET /evil.pdf HTTP/1.1
1598	67.704563	::1	::1	HTTP	1486	HTTP/1.1 200 OK (application/pdf)
1774	75.599414	::1	::1	HTTP	403	GET /atm-image.jpg HTTP/1.1
1796	75.906854	::1	::1	HTTP	352	HTTP/1.1 200 OK (JPEG JFIF image)
2085	89.620153	::1	::1	HTTP	617	GET /ANZ_Document.pdf HTTP/1.1
2537	97.648691	::1	::1	HTTP	1284	HTTP/1.1 200 OK (application/pdf)
2662	103.007294	::1	::1	HTTP	618	GET /ANZ_Document2.pdf HTTP/1.1
3522	112.142837	::1	::1	HTTP	744	HTTP/1.1 200 OK (application/pdf)
3683	119.921382	::1	::1	HTTP	398	GET /ANZ1.jpg HTTP/1.1
3861	122.973950	::1	::1	HTTP	1471	HTTP/1.1 200 OK (JPEG JFIF image)
4074	132.661962	::1	::1	HTTP	398	GET /ANZ2.jpg HTTP/1.1
4277	135.366278	::1	::1	HTTP	282	HTTP/1.1 200 OK (JPEG JFIF image)
4462	143.793646	::1	::1	HTTP	584	GET /broken.png HTTP/1.1
4476	143.999793	::1	::1	HTTP	1020	HTTP/1.1 200 OK (image/png)
4616	150.748121	::1	::1	HTTP	614	GET /securepdf.pdf HTTP/1.1
5575	164.509469	::1	::1	HTTP	554	HTTP/1.1 200 OK (application/pdf)



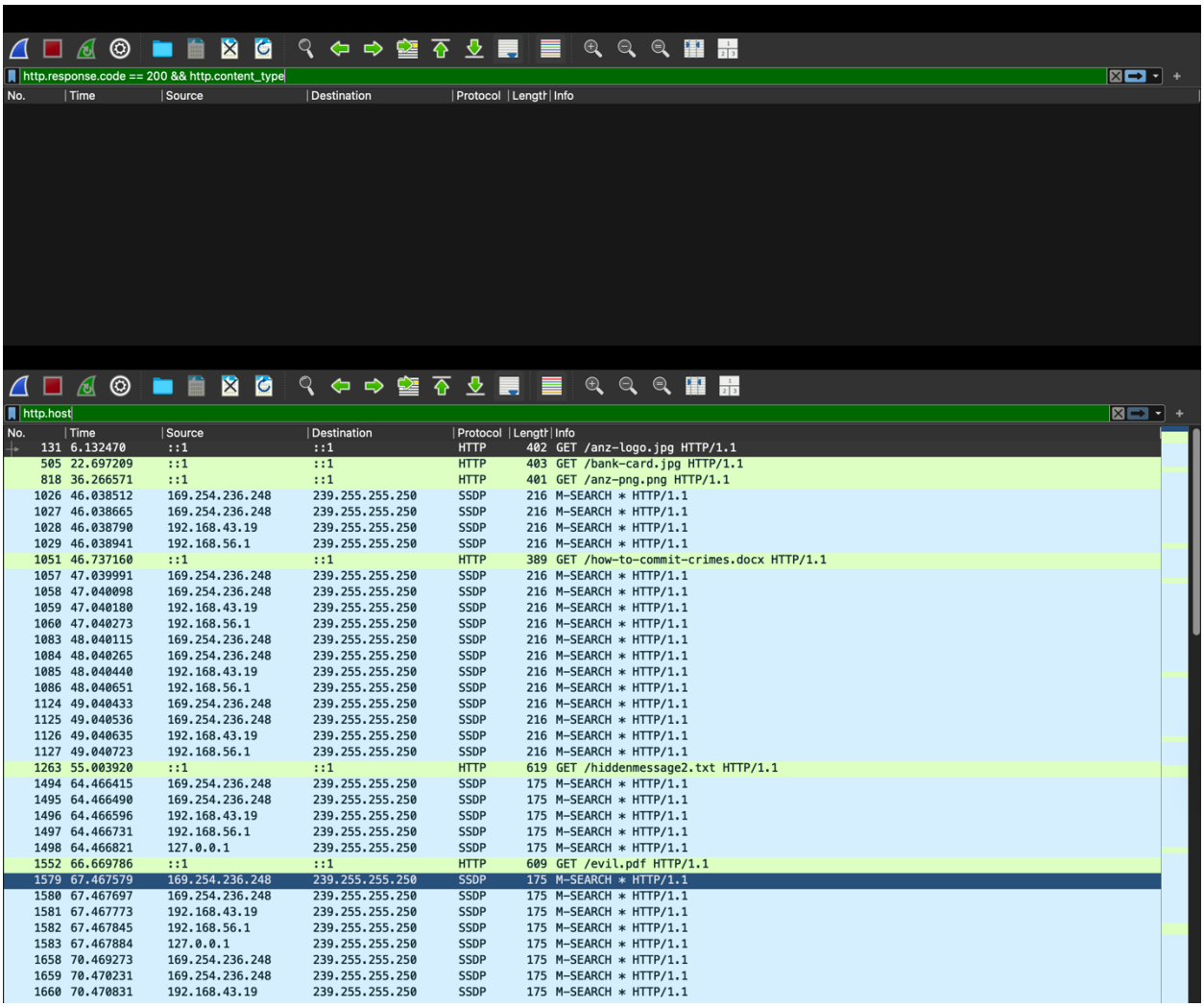
http.request.method== "GET"

No.	Time	Source	Destination	Protocol	Length	Info
131	6.132470	::1	::1	HTTP	402	GET /anz-logo.jpg HTTP/1.1
505	22.697209	::1	::1	HTTP	403	GET /bank-card.jpg HTTP/1.1
818	36.266571	::1	::1	HTTP	401	GET /anz-png.png HTTP/1.1
1051	46.737160	::1	::1	HTTP	389	GET /how-to-commit-crimes.docx HTTP/1.1
1263	55.003920	::1	::1	HTTP	619	GET /hiddenmessage2.txt HTTP/1.1
1552	66.669786	::1	::1	HTTP	609	GET /evil.pdf HTTP/1.1
1774	75.599414	::1	::1	HTTP	403	GET /atm-image.jpg HTTP/1.1
2085	89.620153	::1	::1	HTTP	617	GET /ANZ_Document.pdf HTTP/1.1
2662	103.007294	::1	::1	HTTP	618	GET /ANZ_Document2.pdf HTTP/1.1
3683	119.921382	::1	::1	HTTP	398	GET /ANZ1.jpg HTTP/1.1
4074	132.661962	::1	::1	HTTP	398	GET /ANZ2.jpg HTTP/1.1
4462	143.793646	::1	::1	HTTP	584	GET /broken.png HTTP/1.1
4616	150.748121	::1	::1	HTTP	614	GET /securepdf.pdf HTTP/1.1



http.request.method== "POST"

No.	Time	Source	Destination	Protocol	Length	Info

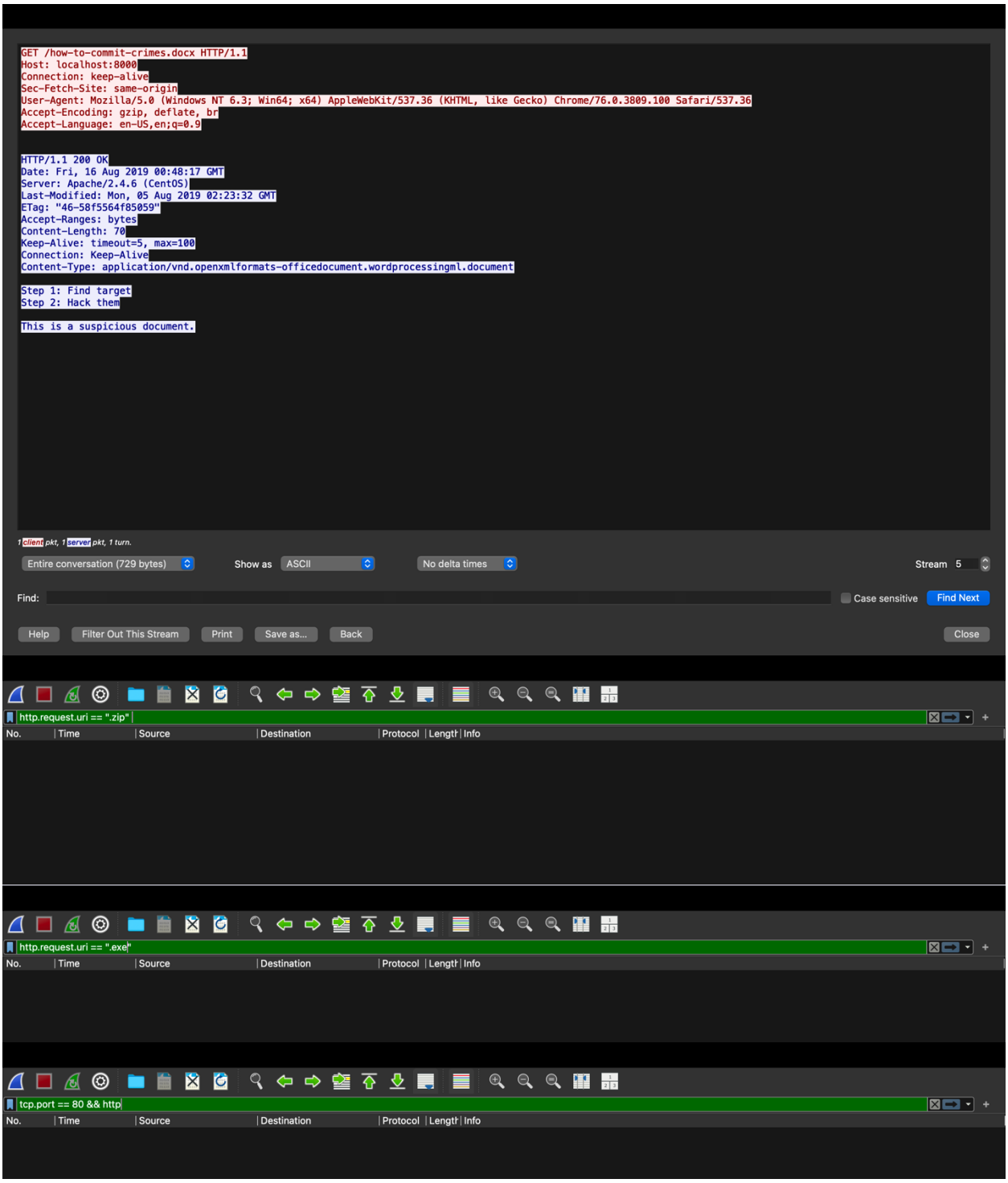


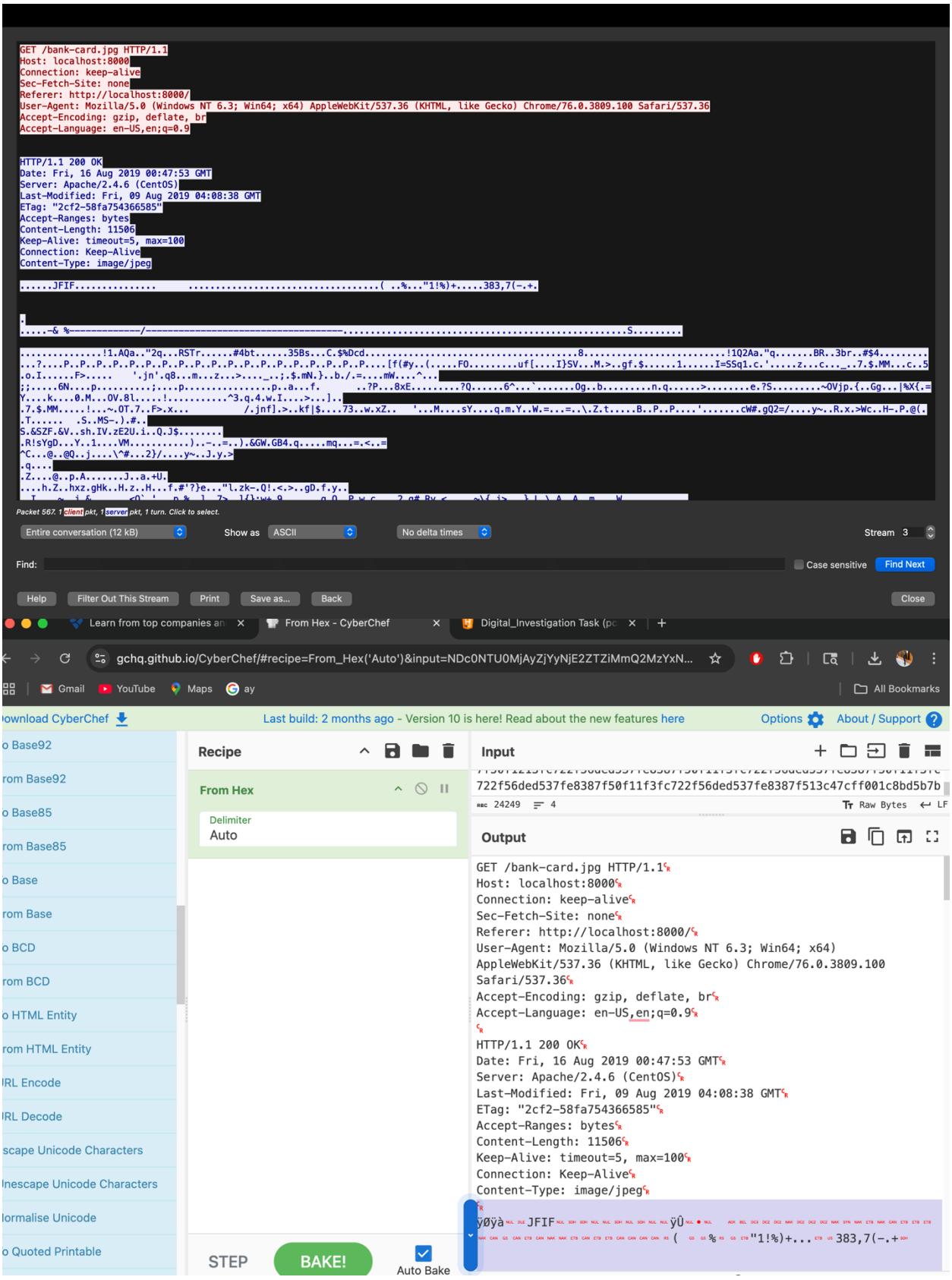
http.response.code == 200 && http.content_type

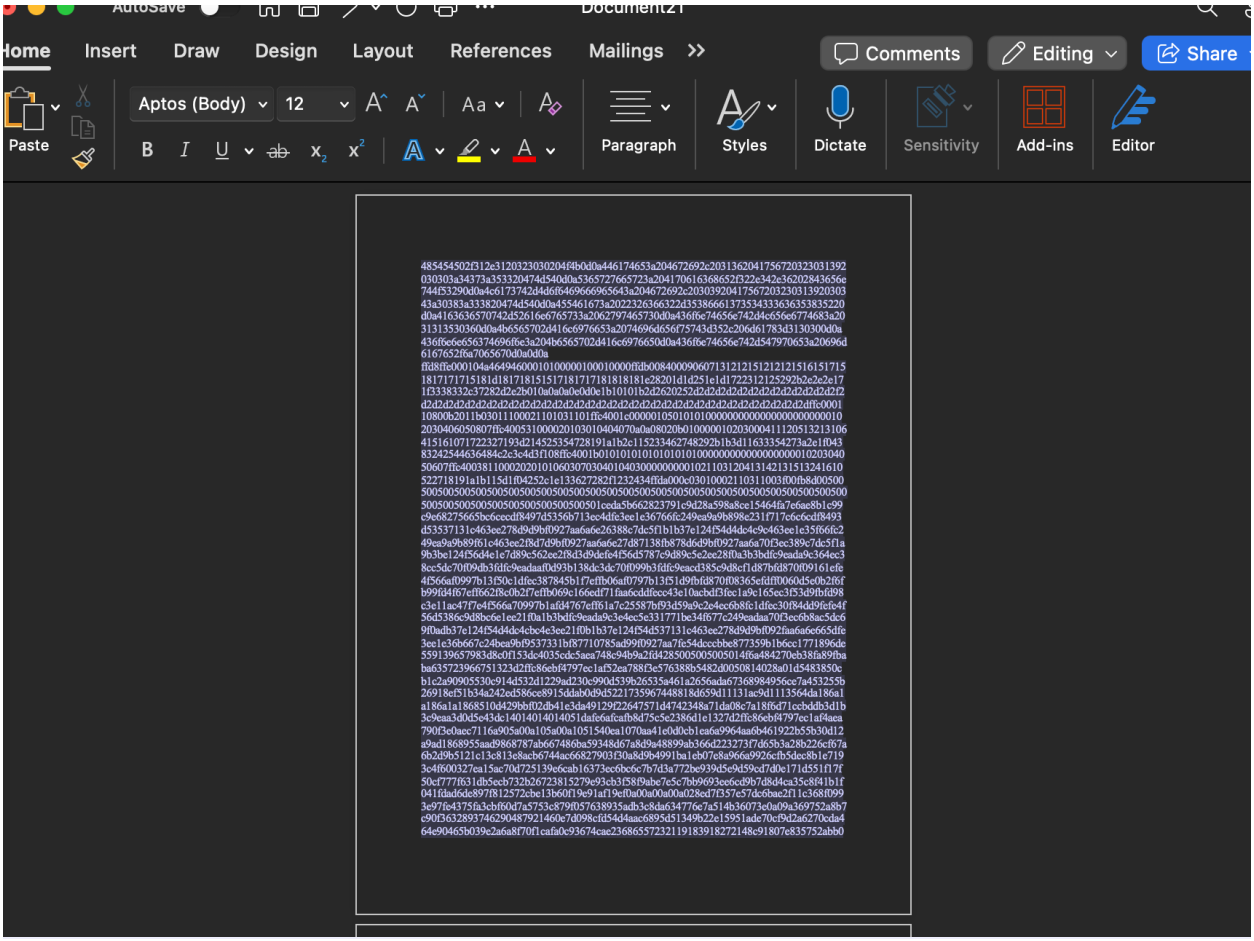
No.	Time	Source	Destination	Protocol	Length	Info

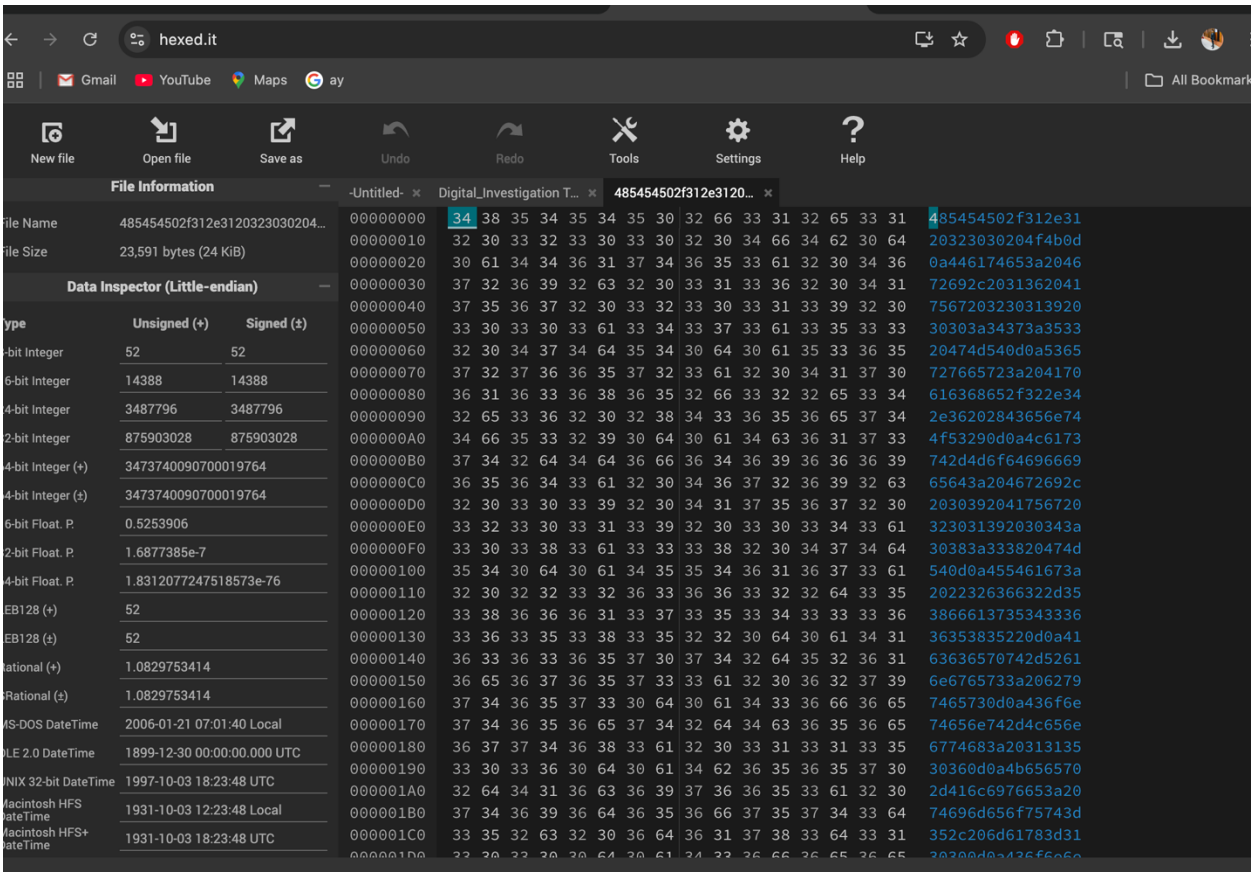
http.host

No.	Time	Source	Destination	Protocol	Length	Info
131	6.132470	::1	::1	HTTP	402	GET /anz-logo.jpg HTTP/1.1
505	22.697209	::1	::1	HTTP	403	GET /bank-card.jpg HTTP/1.1
818	36.266571	::1	::1	HTTP	401	GET /anz-png.png HTTP/1.1
1026	46.038512	169.254.236.248	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1027	46.038665	169.254.236.248	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1028	46.038790	192.168.43.19	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1029	46.038941	192.168.56.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1051	46.737160	::1	::1	HTTP	389	GET /how-to-commit-crimes.docx HTTP/1.1
1057	47.039991	169.254.236.248	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1058	47.040098	169.254.236.248	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1059	47.040180	192.168.43.19	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1060	47.040273	192.168.56.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1083	48.040115	169.254.236.248	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1084	48.040265	169.254.236.248	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1085	48.040440	192.168.43.19	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1086	48.040651	192.168.56.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1124	49.040433	169.254.236.248	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1125	49.040536	169.254.236.248	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1126	49.040635	192.168.43.19	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1127	49.040723	192.168.56.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1263	55.003920	::1	::1	HTTP	619	GET /hiddenmessage2.txt HTTP/1.1
1494	64.466415	169.254.236.248	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1495	64.466490	169.254.236.248	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1496	64.466596	192.168.43.19	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1497	64.466731	192.168.56.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1498	64.466821	127.0.0.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1552	66.669786	::1	::1	HTTP	609	GET /evil.pdf HTTP/1.1
1579	67.467579	169.254.236.248	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1580	67.467697	169.254.236.248	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1581	67.467773	192.168.43.19	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1582	67.467845	192.168.56.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1583	67.467884	127.0.0.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1658	70.469273	169.254.236.248	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1659	70.470231	169.254.236.248	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1660	70.470831	192.168.43.19	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1


GET /how-to-commit-crimes.docx HTTP/1.1
Host: localhost:8000
Connection: keep-alive
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
HTTP/1.1 200 OK
Date: Fri, 16 Aug 2019 00:48:17 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Mon, 05 Aug 2019 02:23:32 GMT
ETag: "46-58f5564f85059"
Accept-Ranges: bytes
Content-Length: 70
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document
Step 1: Find target
Step 2: Hack them
This is a suspicious document.
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (729 bytes)
Show as
ASCII
No delta times
Stream
5
Find:
Case sensitive
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close
http.request.uri == ".zip"
No.
Time
Source
Destination
Protocol
Lengtr
Info
http.request.uri == ".exe"
No.
Time
Source
Destination
Protocol
Lengtr
Info
tcp.port == 80 && http
No.
Time
Source
Destination
Protocol
Lengtr
Info


GET /bank-card.jpg HTTP/1.1
Host: localhost:8000
Connection: keep-alive
Sec-Fetch-Site: none
Referer: http://localhost:8000/
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
HTTP/1.1 200 OK
Date: Fri, 16 Aug 2019 00:47:53 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Fri, 09 Aug 2019 04:08:38 GMT
ETag: "2cf2-58fa754366585"
Accept-Ranges: bytes
Content-Length: 11506
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg
Packet 567. 1 client pkt, 1 server pkt, 1 turn. Click to select.
Entire conversation (12 kB)
Show as
ASCII
No delta times
Stream 3
Find:
Case sensitive
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close
Learn from top companies ar
From Hex - CyberChef
Digital_Investigation Task (pc
gchq.github.io/CyberChef/#recipe=From_Hex('Auto')&input=NDc0NTU0MjAyZjYyNjE2ZTZiMmQ2MzYxN...
Gmail
YouTube
Maps
ay
All Bookmarks
ownload CyberChef
Last build: 2 months ago - Version 10 is here! Read about the new features here
Options
About / Support
o Base92
rom Base92
o Base85
rom Base85
o Base
rom Base
o BCD
rom BCD
o HTML Entity
rom HTML Entity
RL Encode
RL Decode
scape Unicode Characters
nescape Unicode Characters
ormalise Unicode
o Quoted Printable
Recipe
From Hex
Delimiter
Auto
Input
722f56ded537fe8387f50f11f3fc722f56ded537fe8387f513c47cff001c8bd5b7b
24249
4
Raw Bytes
LF
Output
GET /bank-card.jpg HTTP/1.1
Host: localhost:8000
Connection: keep-alive
Sec-Fetch-Site: none
Referer: http://localhost:8000/
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100
Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
HTTP/1.1 200 OK
Date: Fri, 16 Aug 2019 00:47:53 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Fri, 09 Aug 2019 04:08:38 GMT
ETag: "2cf2-58fa754366585"
Accept-Ranges: bytes
Content-Length: 11506
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg
ÿØÿà JFIF ÿÛ "1!%)+... 383,7(-.+
STEP
BAKE!
Auto Bake


AutoSave
Document21
Home
Insert
Draw
Design
Layout
References
Mailings
Comments
Editing
Share
Paste
Aptos (Body)
12
Paragraph
Styles
Dictate
Sensitivity
Add-ins
Editor


hexed.it
Gmail
YouTube
Maps
ay
All Bookmark
New file
Open file
Save as
Undo
Redo
Tools
Settings
Help
File Information
File Name
485454502f312e3120323030204...
File Size
23,591 bytes (24 KiB)
Data Inspector (Little-endian)
Type
Unsigned (+)
Signed (±)
-bit Integer
52
52
6-bit Integer
14388
14388
4-bit Integer
3487796
3487796
2-bit Integer
875903028
875903028
4-bit Integer (+)
3473740090700019764
4-bit Integer (±)
3473740090700019764
6-bit Float. P.
0.5253906
2-bit Float. P.
1.6877385e-7
4-bit Float. P.
1.8312077247518573e-76
EB128 (+)
52
EB128 (±)
52
ational (+)
1.0829753414
Rational (±)
1.0829753414
MS-DOS DateTime
2006-01-21 07:01:40 Local
LE 2.0 DateTime
1899-12-30 00:00:00.000 UTC
UNIX 32-bit DateTime
1997-10-03 18:23:48 UTC
Macintosh HFS DateTime
1931-10-03 12:23:48 Local
Macintosh HFS+ DateTime
1931-10-03 18:23:48 UTC
-Untitled-
Digital_Investigation T...
485454502f312e3120...
00000000 34 38 35 34 35 34 35 30 32 66 33 31 32 65 33 31 485454502f312e31
00000010 32 30 33 32 33 30 33 30 32 30 34 66 34 62 30 64 20323030204f4b0d
00000020 30 61 34 34 36 31 37 34 36 35 33 61 32 30 34 36 0a446174653a2046
00000030 37 32 36 39 32 63 32 30 33 31 33 36 32 30 34 31 72692c2031362041
00000040 37 35 36 37 32 30 33 32 33 30 33 31 33 39 32 30 7567203230313920
00000050 33 30 33 30 33 61 33 34 33 37 33 61 33 35 33 33 30303a34373a3533
00000060 32 30 34 37 34 64 35 34 30 64 30 61 35 33 36 35 20474d540d0a5365
00000070 37 32 37 36 36 35 37 32 33 61 32 30 34 31 37 30 727665723a204170
00000080 36 31 36 33 36 38 36 35 32 66 33 32 32 65 33 34 616368652f322e34
00000090 32 65 33 36 32 30 32 38 34 33 36 35 36 65 37 34 2e36202843656e74
000000A0 34 66 35 33 32 39 30 64 30 61 34 63 36 31 37 33 4f53290d0a4c6173
000000B0 37 34 32 64 34 64 36 66 36 34 36 39 36 36 36 39 742d4d6f64696669
000000C0 36 35 36 34 33 61 32 30 34 36 37 32 36 39 32 63 65643a204672692c
000000D0 32 30 33 30 33 39 32 30 34 31 37 35 36 37 32 30 2030392041756720
000000E0 33 32 33 30 33 31 33 39 32 30 33 30 33 34 33 61 323031392030343a
000000F0 33 30 33 38 33 61 33 33 33 38 32 30 34 37 34 64 30383a333820474d
00000100 35 34 30 64 30 61 34 35 35 34 36 31 36 37 33 61 540d0a455461673a
00000110 32 30 32 32 33 32 36 33 36 36 33 32 32 64 33 35 2022326366322d35
00000120 33 38 36 36 36 31 33 37 33 35 33 34 33 33 33 36 3866613735343336
00000130 33 36 33 35 33 38 33 35 32 32 30 64 30 61 34 31 36353835220d0a41
00000140 36 33 36 33 36 35 37 30 37 34 32 64 35 32 36 31 63636570742d5261
00000150 36 65 36 37 36 35 37 33 33 61 32 30 36 32 37 39 6e6765733a206279
00000160 37 34 36 35 37 33 30 64 30 61 34 33 36 66 36 65 7465730d0a436f6e
00000170 37 34 36 35 36 65 37 34 32 64 34 63 36 35 36 65 74656e742d4c656e
00000180 36 37 37 34 36 38 33 61 32 30 33 31 33 31 33 35 6774683a20313135
00000190 33 30 33 36 30 64 30 61 34 62 36 35 36 35 37 30 30360d0a4b656570
000001A0 32 64 34 31 36 63 36 39 37 36 36 35 33 61 32 30 2d416c6976653a20
000001B0 37 34 36 39 36 64 36 35 36 66 37 35 37 34 33 64 74696d656f75743d
000001C0 33 35 32 63 32 30 36 64 36 31 37 38 33 64 33 31 352c206d61783d31

✅ Conclusion & Reflection

This investigation showcased my ability to handle ambiguous threat intel using layered analysis techniques. Despite tool limitations, I persistently explored multiple pivot points and translated vague network signals into meaningful forensic leads.

My approach mirrored real-world Tier 1/2 SOC operations — from detection and protocol analysis to manual artifact recovery and MITRE mapping. This project proves I'm prepared to contribute immediately in a SOC analyst or junior threat hunter role, with hands-on fluency in Wireshark, investigative logic, and a clear understanding of adversary TTPs.