Cyber Forensics CTF

Jordan Synodis

Scenario

Suspicious behavior was detected on an internal workstation belonging to Jordan Blake (IP: 192.168.1.100). Network logs show FTP activity to an external server (203.0.113.10). Analysts believe a covert message was transmitted. Can you uncover this message?

PCAP File

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.121	142.250.69.128	TCP	70	49225 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
2	0.000224	192.168.1.35	142.250.69.7	TCP	70	58624 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
3	0.000380	192.168.1.55	142.250.69.55	TCP	70	49260 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
4	0.000546	192.168.1.175	142.250.69.103	TCP	70	60749 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
5	0.000696	192.168.1.54	142.250.69.22	TCP	70	51092 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
6	0.000851	192.168.1.150	142.250.69.208	TCP	70	51608 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
7	0.000999	192.168.1.165	142.250.69.56	TCP	70	49833 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
8	0.001148	192.168.1.167	142.250.69.1	TCP	70	54395 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
9	0.001303	192.168.1.165	142.250.69.111	TCP	70	50420 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
10	0.001454	192.168.1.120	142.250.69.219	TCP	70	65200 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
11	0.001602	192.168.1.75	142.250.69.73	TCP	70	54934 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
12	0.001764	192.168.1.162	142.250.69.211	TCP	70	50720 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
13	0.001923	192.168.1.10	142.250.69.251	TCP	70	60838 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
14	0.002071	192.168.1.175	142.250.69.26	TCP	70	57088 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
15	0.002219	192.168.1.104	142.250.69.68	TCP	70	63471 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
16	0.002379	192.168.1.17	142.250.69.40	TCP	70	65009 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
17	0.002527	192.168.1.96	142.250.69.94	TCP	70	53758 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
18	0.002674	192.168.1.83	142.250.69.60	TCP	70	50911 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
19	0.002825	192.168.1.131	142.250.69.141	TCP	70	53117 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
20	0.002980	192.168.1.138	142.250.69.23	TCP	70	62052 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
21	0.003133	192.168.1.160	142.250.69.182	TCP	70	53560 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
22	0.003281	192.168.1.122	142.250.69.248	TCP	70	51548 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
23	0.003429	192.168.1.104	142.250.69.93	TCP	70	53811 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
24	0.003577	192.168.1.124	142.250.69.159	TCP	70	50416 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
25	0.003724	192.168.1.35	142.250.69.194	TCP	70	57266 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
26	0.003905	192.168.1.82	142.250.69.223	TCP	70	63085 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
27	0.004052	192.168.1.123	142.250.69.44	TCP	70	64916 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
28	0.004219	192.168.1.122	142.250.69.77	TCP	70	65388 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
29	0.004365	192.168.1.49	142.250.69.149	TCP	70	62625 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16
30	0.004513	192.168.1.139	142.250.69.57	TCP	70	56424 → 80 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=16

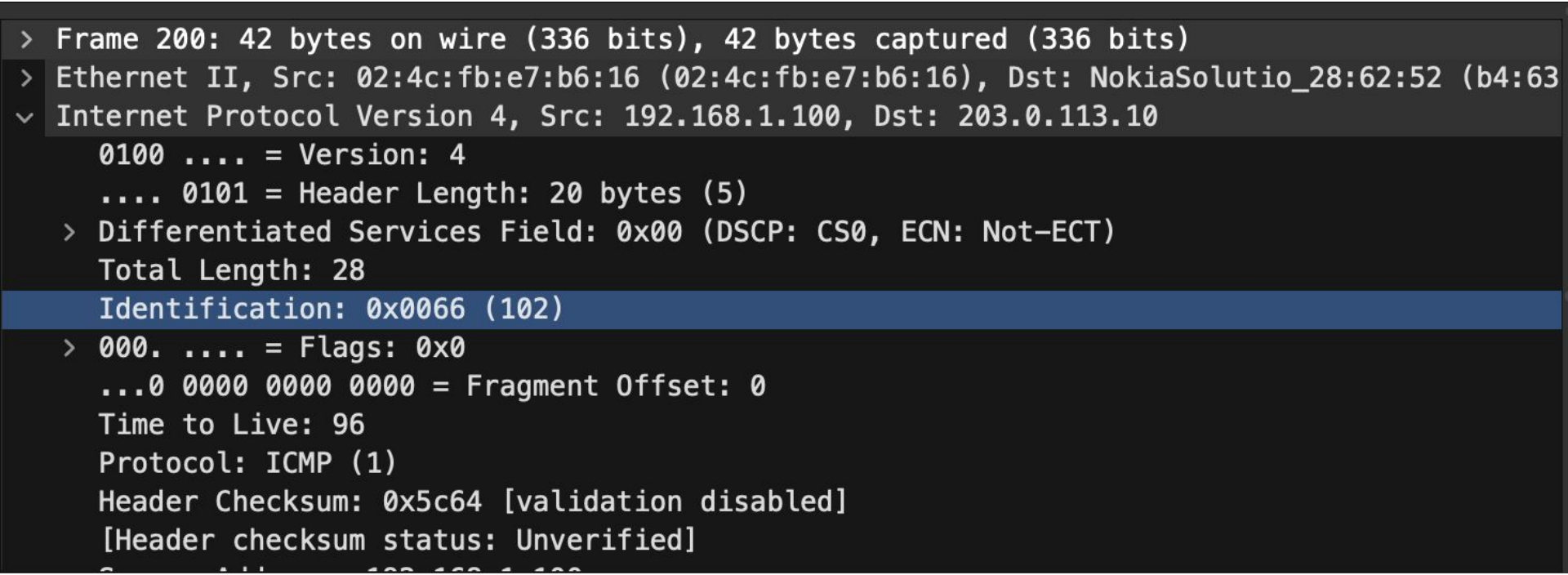
Sorted Dest IP

102	0.015521	192.168.1.100	203.0.113.10	FTP	67	Request: USER jordan
104	0.015819	192.168.1.100	203.0.113.10	FTP	71	[TCP ACKed unseen segment] [TCP Previous segment not captured] Request: PASS s3cr3tP@ss
106	0.016118	192.168.1.100	203.0.113.10	FTP	59	[TCP ACKed unseen segment] [TCP Previous segment not captured] Request: PWD
108	0.016550	192.168.1.100	203.0.113.10	FTP	60	[TCP ACKed unseen segment] [TCP Previous segment not captured] Request: SYST
110	0.016854	192.168.1.100	203.0.113.10	FTP	60	[TCP ACKed unseen segment] [TCP Previous segment not captured] Request: HELP
112	0.017156	192.168.1.100	203.0.113.10	FTP	60	[TCP ACKed unseen segment] [TCP Previous segment not captured] Request: QUIT
200	0.030545	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=96 (no response found!)
201	0.030727	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=62 (no response found!)
202	0.030862	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=87 (no response found!)
203	0.030992	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=63 (no response found!)
204	0.031120	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=85 (no response found!)
205	0.031256	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=109 (no response found!)
206	0.031382	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=61 (no response found!)
207	0.031511	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=106 (no response found!)
208	0.031638	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=111 (no response found!)
209	0.031763	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=73 (no response found!)
210	0.031890	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=100 (no response found!)
211	0.032015	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=106 (no response found!)
212	0.032138	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=124 (no response found!)
213	0.032261	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=127 (no response found!)
214	0.032387	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=62 (no response found!)
215	0.032523	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=105 (no response found!)
216	0.032652	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=71 (no response found!)
217	0.032798	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=81 (no response found!)
218	0.032924	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=119 (no response found!)
219	0.033049	192.168.1.100	203.0.113.10	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=106 (no response found!)

Follow TCP Stream

```
220 FTP Server ready.

USER jordan

[13 bytes missing in capture file].331 Password required for jordan

[34 bytes missing in capture file].PASS s3cr3tP@ss

[17 bytes missing in capture file].230 User jordan logged in.

[28 bytes missing in capture file].PWD

[5 bytes missing in capture file].257 "/secure/data" is current directory.

[42 bytes missing in capture file].SYST

[6 bytes missing in capture file].215 UNIX Type: L8

[19 bytes missing in capture file].HELP

[6 bytes missing in capture file].214 Special note: Check IP identification fields in packets 200-220 for important values.

[91 bytes missing in capture file].QUIT
```

Find Identification Values



Flag

102 108 97 103 123 99 121 98 51 114 70 48 114 51 110 115 49 99 53 125

flag{cyb3rF0r3ns1c5}