



Wireshark Scan #1



Case Title: FTP-Cleartext Credentials Analysis

Date: July 17, 2025

Session Length: ~3 hours

Analyst: Jinay [a.k.a. *Jynx*]

🧠 Objective

To analyze FTP traffic from a PCAP file and extract cleartext login credentials. Document findings, tools used, and implications for secure protocol usage.

📁 File Metadata

Attribute	Info
📁 File Name	ftp_login.pcap
📦 Source	Download file: [https://www.cloudshark.org/captures/abdc8742488f]
📅 Likely Date of Capture	Unknown (lab-generated)
✍️ Content	Cleartext FTP authentication over TCP
🔍 Size	~60–80 KB

Attribute	Info
💻 Protocols in Use	TCP, FTP (port 21)
📦 Use Case	Beginner protocol analysis & credential extraction
🌐 Source IP	192.168.1.182
🌐 Destination IP	192.168.1.231

🛠️ Tools Used

- Wireshark GUI on Windows 11
- Filters: `ftp`, `ftp.request.command`, `tcp.stream eq 0`
- Follow TCP Stream feature
- Notion for documentation

✍️ Step-by-Step Analysis

1. Opened PCAP in Wireshark
2. Applied display filter: `ftp`
3. Identified FTP login request (`USER`, `PASS`)
4. Right-clicked → Follow → TCP Stream
5. Saw credentials in cleartext:

```
USER ftp
PASS ftp
[Anonymous Login: " 230 Anonymous access granted, restrictions apply.
"]
```

6. Noted IPs, ports, direction of flow
7. Assessed risk (cleartext login can be intercepted)

❗ Findings

- FTP credentials were sent in plain text

No.	Time	Source	Destination	Protocol	Length	Info
6	2.522199	192.168.1.182	192.168.1.231	FTP	76	Request: USER ftp
10	4.098171	192.168.1.182	192.168.1.231	FTP	76	Request: PASS ftp
14	6.071130	192.168.1.182	192.168.1.231	FTP	72	Request: SYST
18	6.071927	192.168.1.182	192.168.1.231	FTP	72	Request: FEAT
23	6.095187	192.168.1.182	192.168.1.231	FTP	71	Request: PWD
27	9.394257	192.168.1.182	192.168.1.231	FTP	72	Request: EPSV
31	9.395696	192.168.1.182	192.168.1.231	FTP	72	Request: LIST
36	17.706270	192.168.1.182	192.168.1.231	FTP	74	Request: TYPE I
39	17.707062	192.168.1.182	192.168.1.231	FTP	83	Request: SIZE resume.doc
42	17.708040	192.168.1.182	192.168.1.231	FTP	72	Request: EPSV
46	17.772178	192.168.1.182	192.168.1.231	FTP	83	Request: RETR resume.doc
52	17.984040	192.168.1.182	192.168.1.231	FTP	83	Request: MDTM resume.doc
56	22.202082	192.168.1.182	192.168.1.231	FTP	79	Request: CWD uploads

```

220 ProFTPD 1.3.0a Server (ProFTPD Anonymous Server) [192.168.1.231]

USER ftp

331 Anonymous login ok, send your complete email address as your password.

PASS ftp

230 Anonymous access granted, restrictions apply.

SYST

215 UNIX Type: L8

```

- No encryption (no TLS/SSL)
- Could very comfortably illustrate the sequence of command operated, could lead to serious security triage or exploit.
- Source IP **192.168.1.182** attempted login to destination **192.168.1.231**

Takeaways

- Legacy protocols like FTP are dangerous
- Wireshark can extract creds in seconds, if outdated or unreliable protocols are still in use or if security patches are not timely updated.
- Proper filtering and stream reconstruction is key