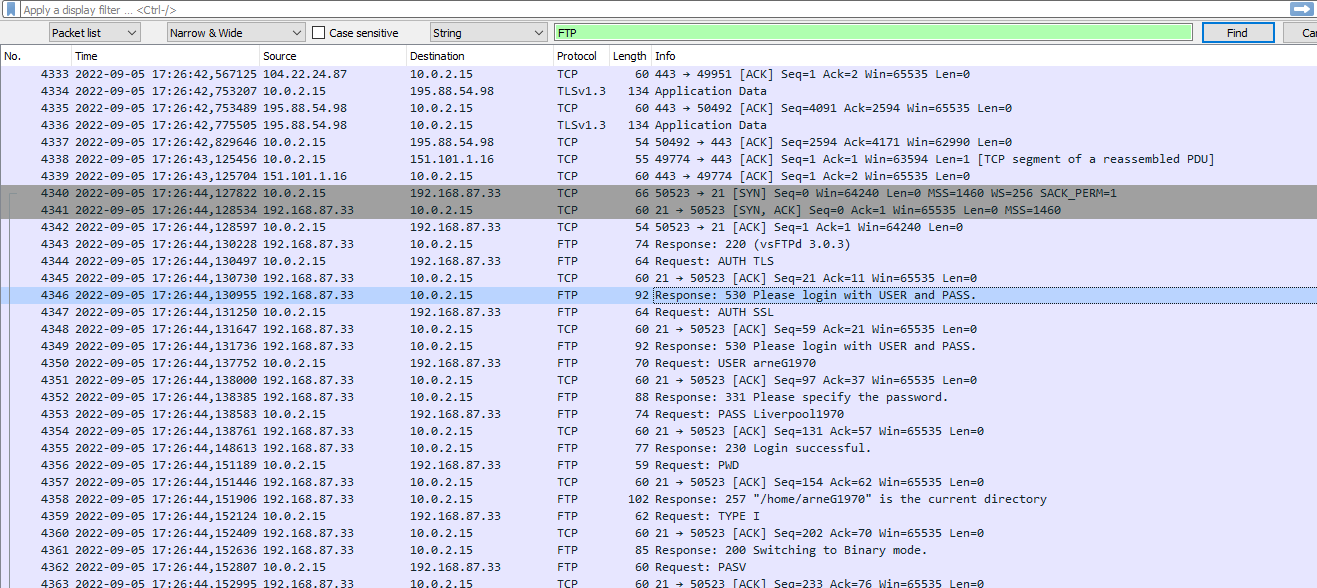
Noen tilleggs spørsmål: Del 1

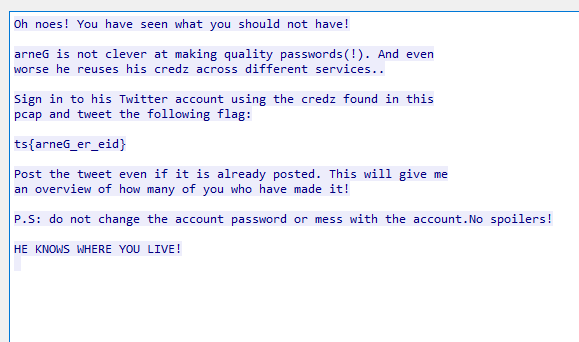
1. **Hva kunne arneG ha gjort for å unngå problematikken? (Det er minst 5 tiltak som kunne stoppet en angriper)**

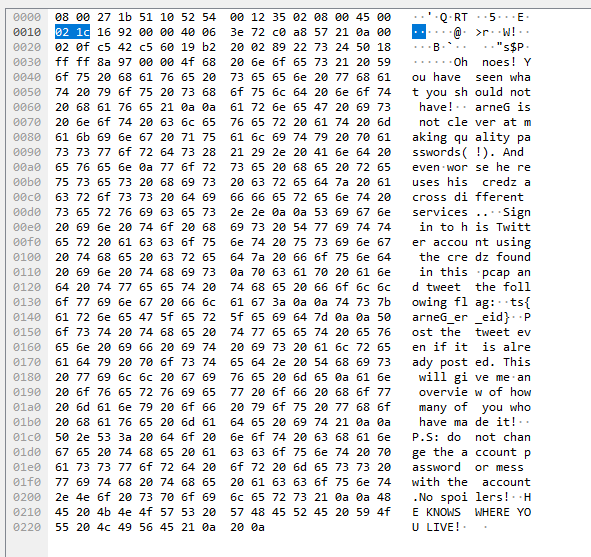
* Han kunne ha brukt totrinnsautorisering
* Han kunne ha brukt kryptering
* Unngå å bruke FTP som viser ting i klartekst
* Bruke SHA-256 kryptering eller AES-256 kryptering
* Unngå gjenbrukte passord



1. **Hvorfor er det så kryptisk det som står i de andre strømmene?**

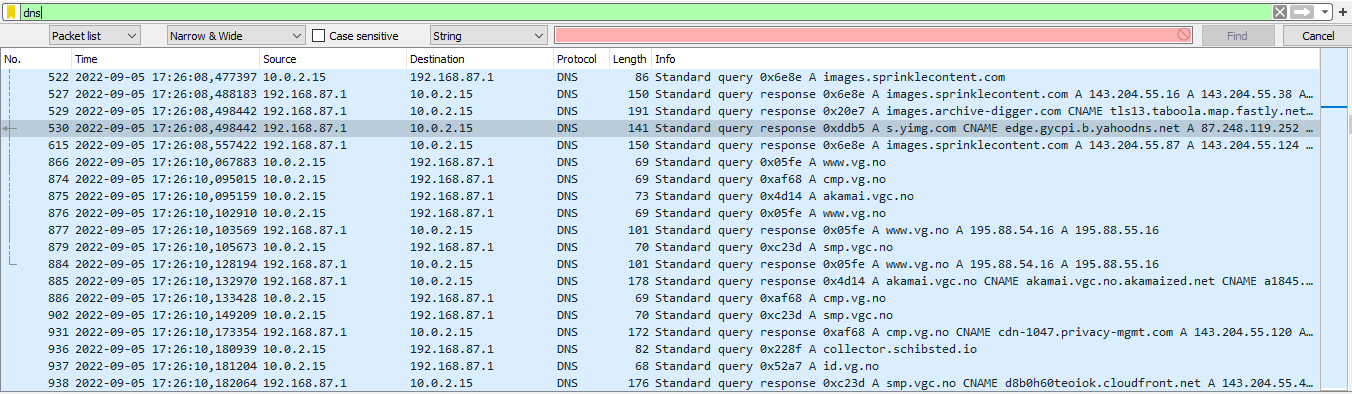
Det er kryptisk fordi det er en fil som består av hemmelig info som ikke skal være synlig for offentligheten.



 For å finne hemmelig tekst filtrer jeg string og skriver secret , deretter trykker jeg på protocol = FTP-Data nr 554 (br:arneg1970 pass=Liverpool1970 eller høyre klikk (tcp stream) follow :

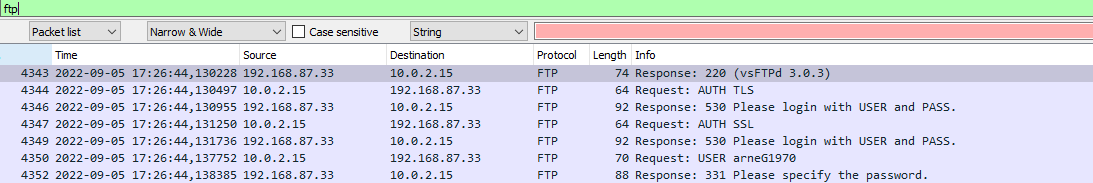
1. **Bruk whois, dig eller noe annet til å finne ut andre steder arneG har besøkt? Hvilken protokoll er dette?**

Skriver dns på wireshark og finner nettsidene han har besøkt: Dette er en DNS protokoll (Domain Name System ) og finner tilsvarende:



1. **Hvilken FTP server er brukt i denne dumpen? Og hvilket OS?**

Søker ftp i wireshark



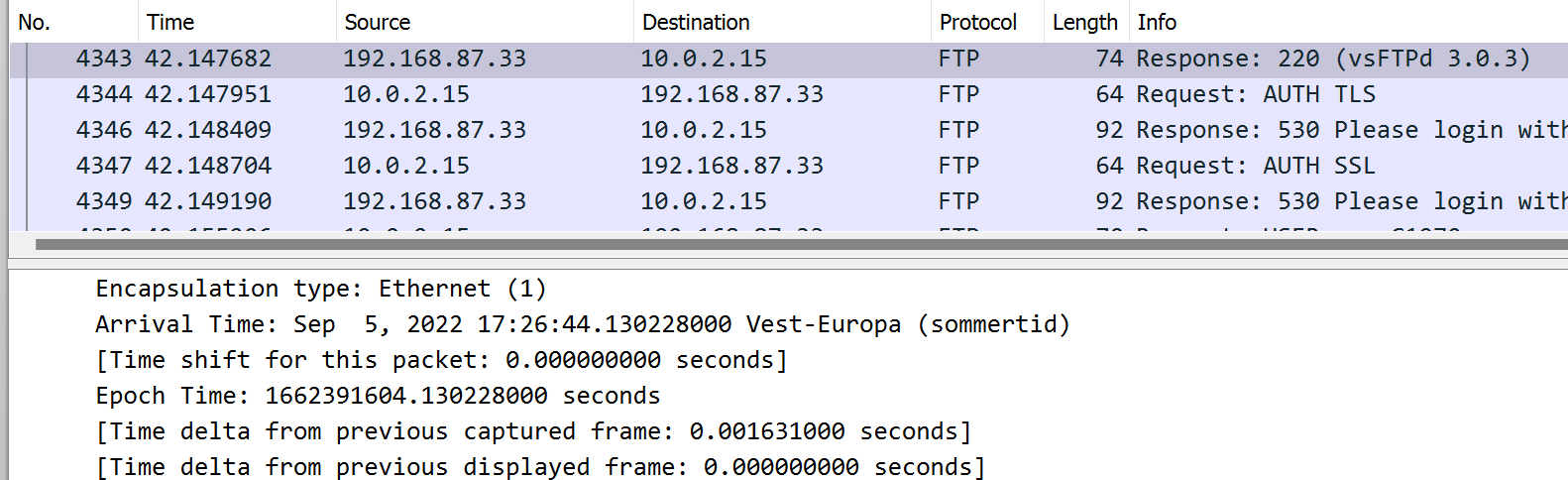
Serveren er : vsFTPd 3.0.3 googler server og finner os = CentOS 7 og blir brukt i rocky linux

<https://www.getpagespeed.com/solutions/would-vsftpd-3-0-3-be-supported-on-centos-7>

1. **Når ble pcapen laget? Finner du noen timestamps?**

Gå på wireshark trykk på statistics og du får opp: den ble laget (22.09.05)

Timestamps er som står øverst på statestikken:



Under epoc time ligger det timestamps

Del 2 :

1. **Klarer du å tidfeste de ulike hendelsene der APT29 har vært involvert og hvilke verktøy de brukte?**

APT29 er en russisk trusselaktør (hacker gruppe) som har vært involvert i saker siden de ble dannet i 2008 og har ofte målrettet seg mot regjeringsnettverket i europa og Nato medlemslandeme , forskningsinstitutter osv.

I 2015 komprommiterte(brutt seg inn) i den nasjonale komiteen

I 2021 kompromiterte APT29 myndighetene , konsulenttjenestene , teknologi , telekom og andre organisasjoner i Nord Amerika , Europa , Asia og Midtøsten

Verktøy de brukte får å få tilgang til nettverket er som VPN og andre fjerntilgangsverktøy som:

* Tjenestekontrollbehandleren ble brukt for å deaktivere forsvarets sikkerhetsovervåkningsprodukter.
* SDelete ble brukt for å fjerne gjenstander fra ofrene.
* TEARDROP
* COLBATSTRIKE
* Mimikatz
* Tor
* Meek
* Kommandolinjeverktøy

1. **Hvilke CVEer har gruppen brukt? Klarer du å spore**

De har brukt :

* CVE-2019-19781 for Citric
* CVE-2018-13379 for FortiGate og VPN-er
* CVE-2019-9670 i Zimba programvaren
* CVE-2020-0688 mot Microsoft Exchange-kontrollpanelet for å få tilbake tilgang til et nettverk

**3. En annen stor og kjent gruppering er APT1. Klarer du å finne likheter og ulikheter ved å sammenligne de to**

**gruppene?**

**Ulikheter:**

* APT 1 er en kinesisk hackergruppe
* APT29 er en russisk hackergruppe
* APT 1 har brukt pass the hash
* APT 1 og APT 29 bruker ulike teknikker for å bryte seg inn i et nettverk
* Tilsvarende for verktøy , APT 29 benytter seg av mye verktøy som Tor og TEARDROP , i mens APT 1 bruke kommandolinjeverktøy for å bryte seg inn i et nettverk
* APT1 var ute etter å stjele sensitiv dokumenter fra ofre , i mens APT29 var mer målrettet mot å sensitiv data fra regjeringene enn dokumenter.

**Felles:**

* De har de har et fellesmål: å bryte seg inn i nettverk. Og få penger.
* Begge har brukt Mimikratz verktøyet.

**4. Ett av målene til APT29 har vært Solarwinds. Finn informasjon om angrepet og forsøk deretter å sett de inn i**

**diamantmodellen. Sluttresultatet tar du vare på i et dokument. Gå gjerne sammen i grupper og sammenlign**

**deres modeller. Har dere kommet frem til samme resultatene?**

**Diamant modellen:**

**Adversary (Motpart):**

* Hacktivist
* Trusselaktører

**Infrastruktur:**

* Domener
* Webtjenester
* VPN infrastruktur

**Offre:**

* Offentlige nettverk
* Regjeringen og tjenester
* Land i Europa , midøsten , asia , Nord Amerika
* Nato medlemsland

**Evner(Capability):**

* Hackerverktøy
* Kommandolinjeverktøy
* Programmer for å utføre de ondsinnede handlingene

**Meta- Features:**

* Timestamp
* Result
* Direction (retning)
* Ressurser

**5. Som sikkerhetsanalytiker i et stort internasjonalt selskap fatter du mistanke om at APT29 har vært inne i deres systemer. Du har gjort en grundig jobb med å kartlegge aktøren ved hjelp av rammeverkene vi har sett på i dag og sist. Hvordan kan du bruke indikatorene du har kartlagt for å følge aktøren og finne flere spor? Forsøk å plassere så mange indikatorer som mulig i forskjellige barrierer! (Her gjelder det å tenke defense-in-depth)**

* Jeg hadde sett etter om selskapet har vært utsatt for spear phishing email
* Jeg hadde sett etter sårbarheter , ved å ha en pentest for eksempel for å sikre systemene mot fremtidige angrep eller spor av angrep
* Se om systemet har blitt rammet av en malware eller lignende ved bruk av en antivirus programvare for å blokkere angriperen fra å få tilgang til systemet.
* Trene opp ansatte til å unngå phishing og sørge for at de har opplæring i sikkerhet for å sikre seg selv på nettet
* Oppdatere systemet er viktig for å tette sikkerhetshull som kan gi hackeren mulig å bryte seg inn i systemet
* Sørge for at filene i selskapet er kryptert slik at det ikke er fare for at hackere for uatorisert tilgang til dem
* Ta backup av systemet i tillfelle hackere forsøker å sabbotere eller modifisere systemet
* Bruke andre sikkerhetsverktøy
* Fysisk sikring som å ha overvåkningskameraer og sikkerhetsvakt burde også prioriteres for det an hende at hackeren er blant de ansatte

1. **Vi skal senere i kurset se nærmere på automatisering av utveksling av indikatorer, men klarer du å finne verktøy for utveksling og automatisering av indikatorer allerede nå?**

* Microsoft IOC Detection Tool for Exchange Server Vulnerabilities er et verktøy
* Powershell