**Fondul Social European**

**Programul Operațional Capital Uman 2014-2020**

Axa prioritară **Educatie si Competente (AP6)**

Prioritatea de investiții: ***10.iv - Sporirea relevanţei pe piaţa forţelor de muncă a educaţiei şi a sistemelor de formare, facilitarea tranziţiei de la educaţie la piaţa forţelor de muncă  şi consolidarea formării  şi a sistemelor de formare profesională, precum şi a calităţii lor, inclusiv prin mecanisme de anticipare a competenţelor, adaptarea programelor de învăţământ şi instituirea şi dezvoltarea unor sisteme de învăţare la locul de muncă, inclusiv a unor sisteme de învăţare duală  şi programe de ucenicie***

Beneficiar: **Universitatea Titu Maiorescu din Bucuresti**

Titlul proiectului: „**STAGII DE PRACTICA IN CENTRUL DE EXCELENTA IN SECURITATE CIBERNETICA IN CLOUD - CyberX**”

Contract de finanțare nr. **24093/ 25.11.2020** Cod SMIS: **133276**

**ACTIVITĂȚI DESFĂȘURATE**

**PE PARCURSUL STAGIULUI DE PRACTICĂ**

***Etapa de lucru pe platforma***

***CENTRUL DE EXCELENTA IN SECURITATE CIBERNETICA IN CLOUD – CyberX***

**Lucrări practice**

**STUDENT:**

**.............Parfion Vladut.........**

# Acces la platforma laborator - Symantec:

User name: student6

Password:

# COMPONENTA 4 – Symantec Security Analytics v. 8.2.1

1. **Metoda de acces**:

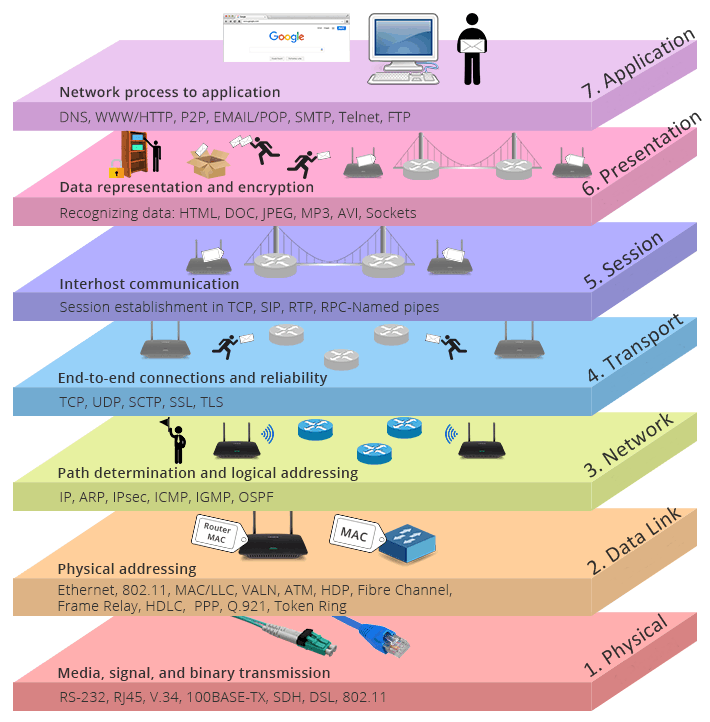
**User name:**

**Password:**

Atacurile avansate sunt de cele mai multe ori direcționate, programele malware sunt personalizate se infiltrează în rețele la viteze record.

Tradițional soluțiile de securitate pur și simplu nu țin pasul. De fapt, recent rapoartele indică faptul că marea majoritate a atacurilor au compromis țintele lor în câteva ore, minute, chiar secunde, în timp ce 75% din atacuri durează zile, luni, chiar și ani înainte de a fi descoperite și anihilate.

Symantec are o soluție. Symantec Security Analytics, oferă vizibilitate deplină, analiza de securitate, informații despre amenințări în timp real și un sistem de înregistrare al activității suspecte, astfel încât să descoperiți cu succes atacurile informatice avansate pentru a va proteja infrastructura.

Aceste lucruri se fac prin captură completă a traficului de rețea, pe nivelele 2-7, vă oferă informații în tot traficul de rețea, inclusiv în comunicații între aplicațiile care rulează în rețelele dvs. virtuale;

Acest trafic este ulterior indexat, clasificat si analizat pentru a se detecta si raporta orice anomalie.

Cum se retine: **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing

Sau: **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

Modul in care acest trafic este interpretat.

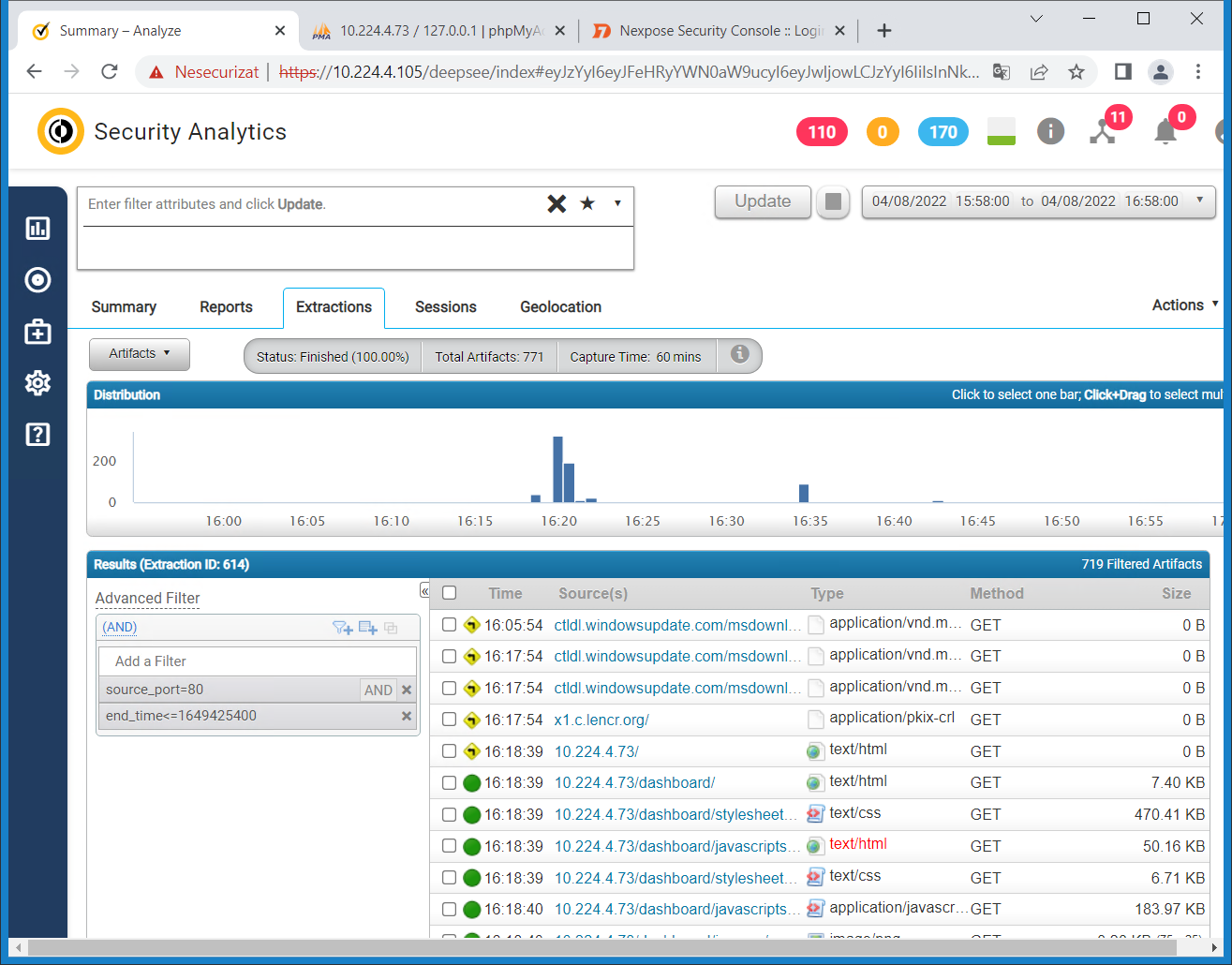
Aici 🡪Graphical user interface, application

Description automatically generated se află configurările pentru “îmbogățirea traficului”

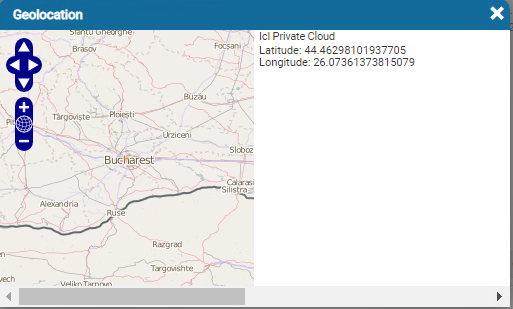
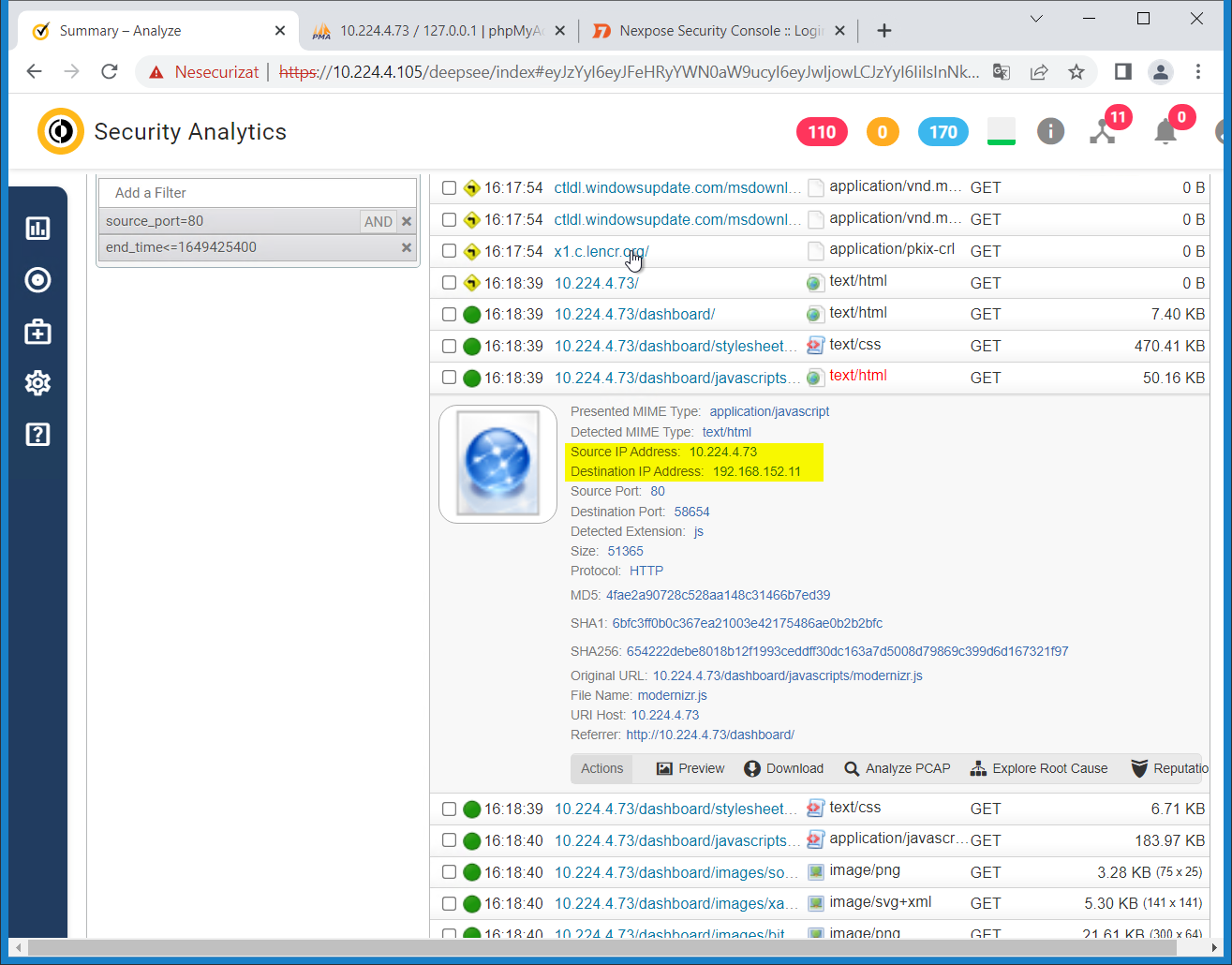
Data Enrichment: <https://10.224.4.105/integration_providers/index>

**Sa se analizeze 60 minute din traficul real capturat astfel incat:**

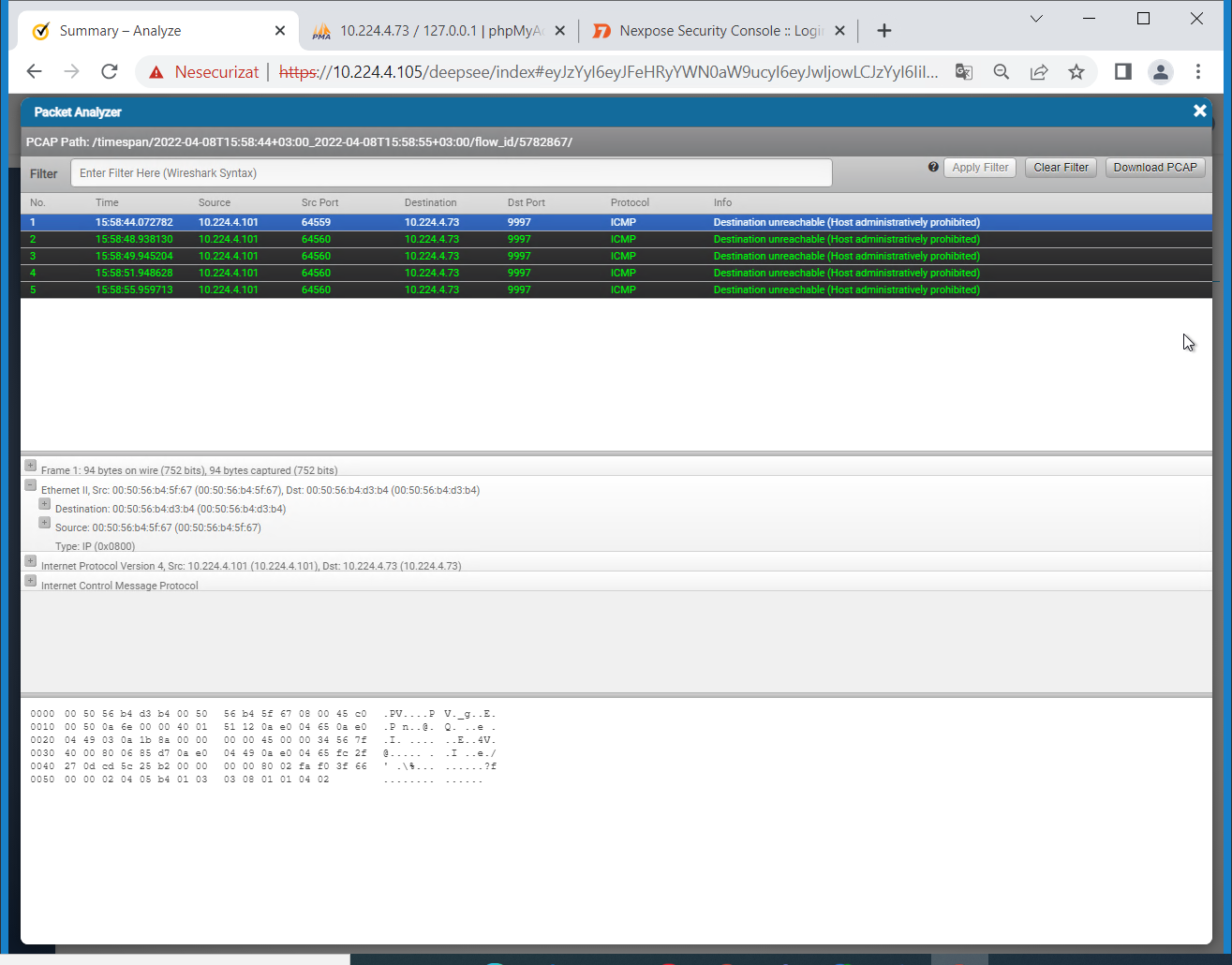
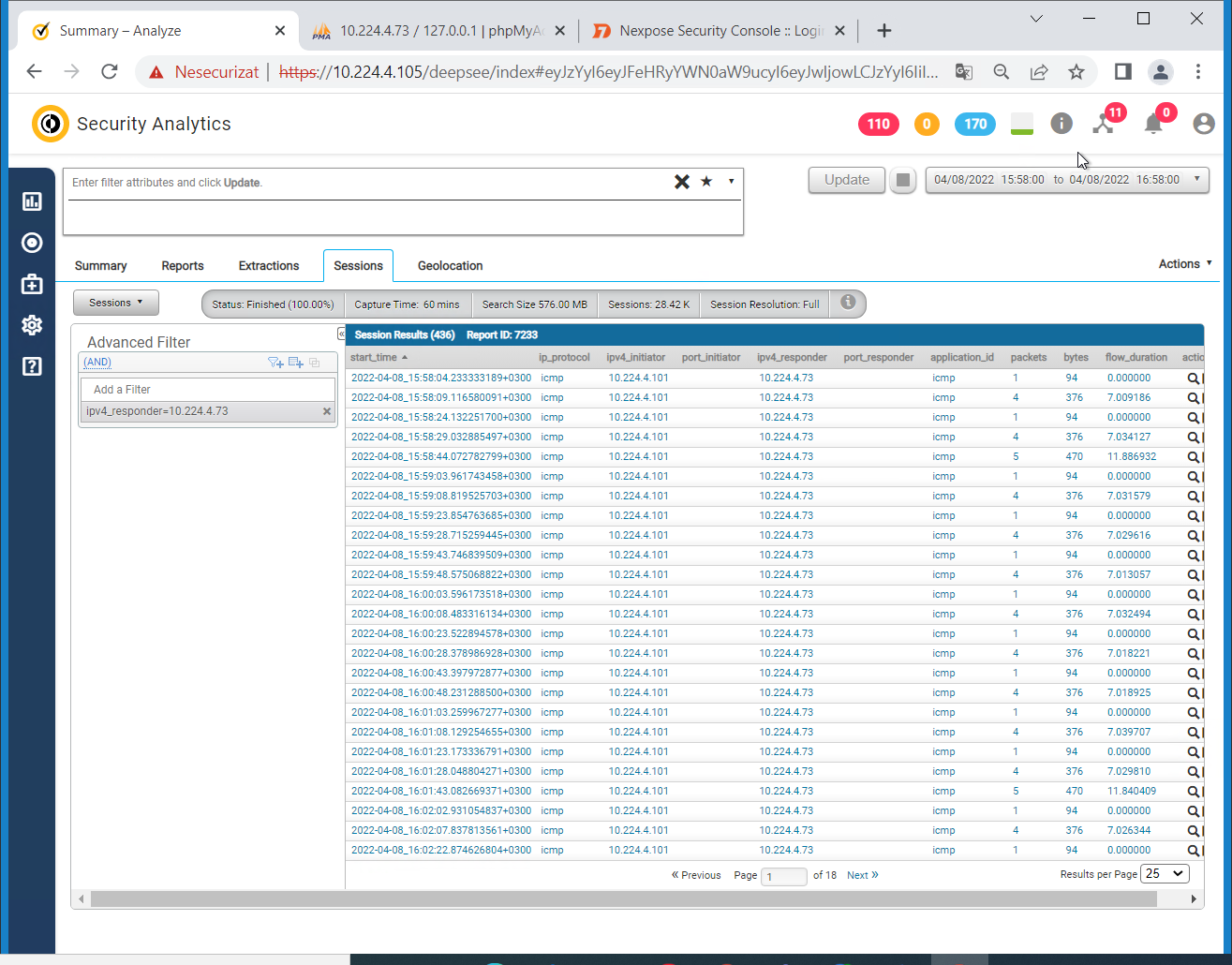
Obtineti artefactele care au portul source 80 (Extraction  source\_port=80);



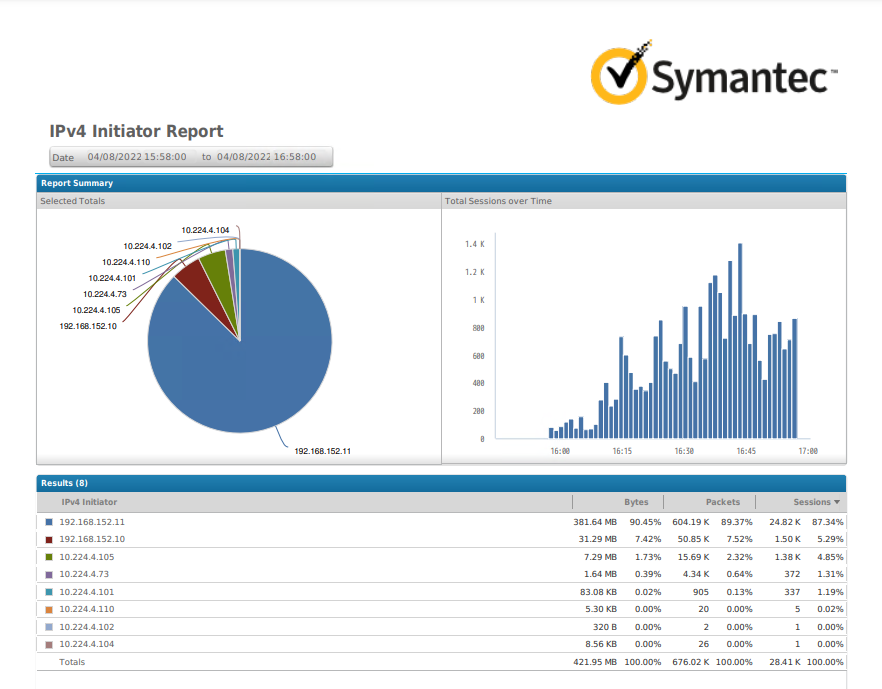
identificati IP-ul sursa/destinatie si geolocatia pentru aceste artefacte;

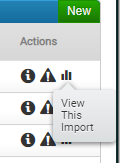


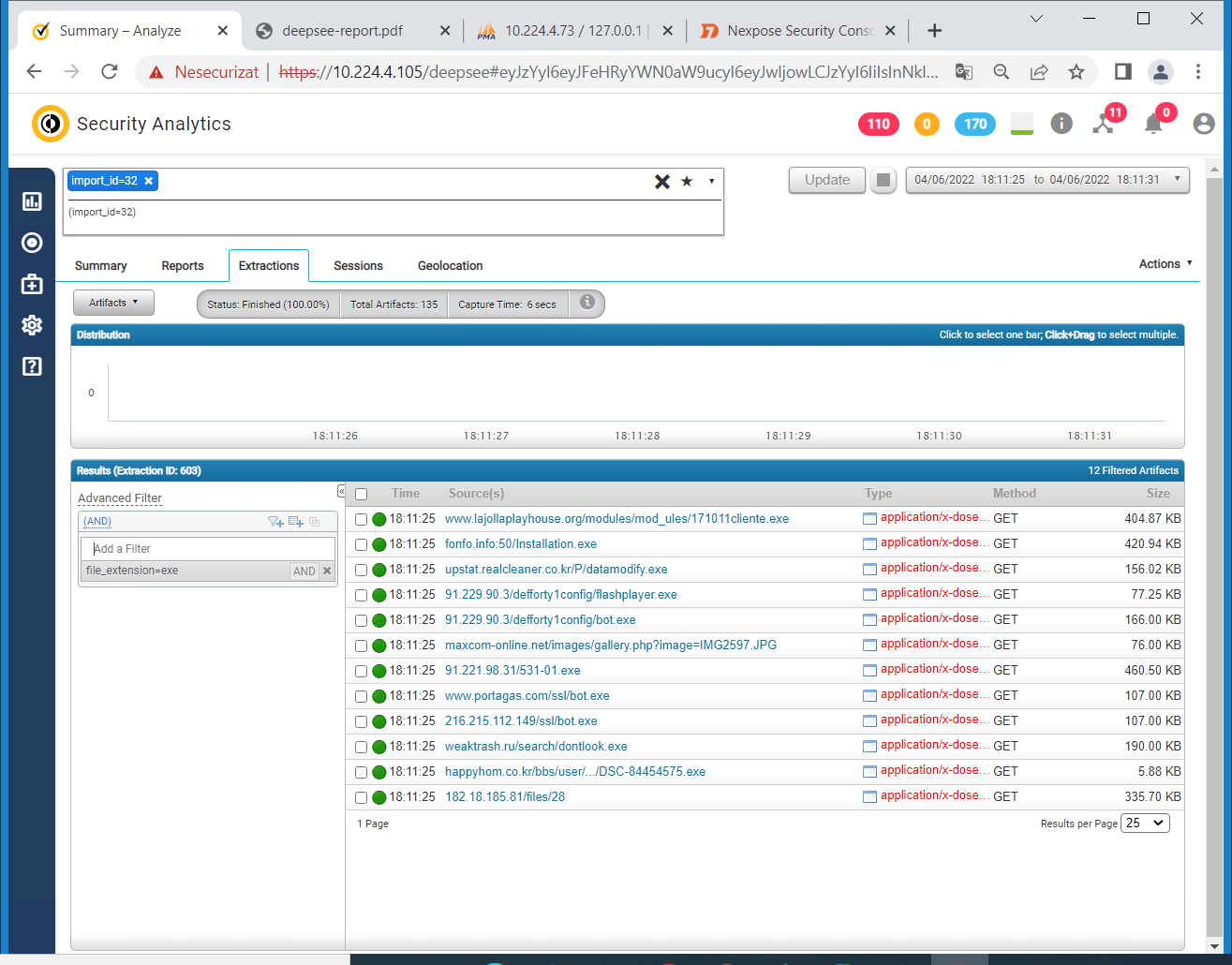
Analizati Destination IP Address: 10.224.4.73 (Session ipv4\_responder=10.224.4.73);



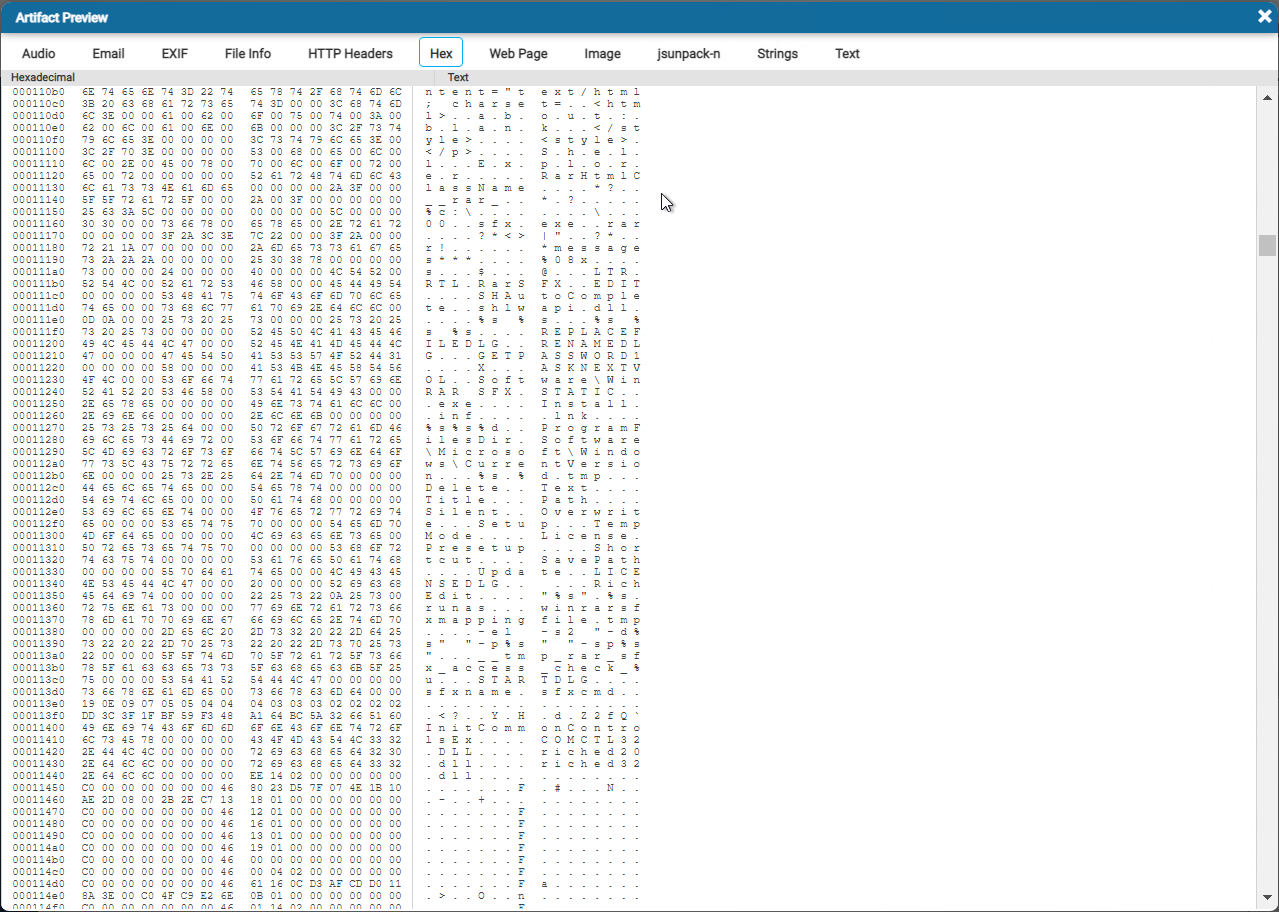
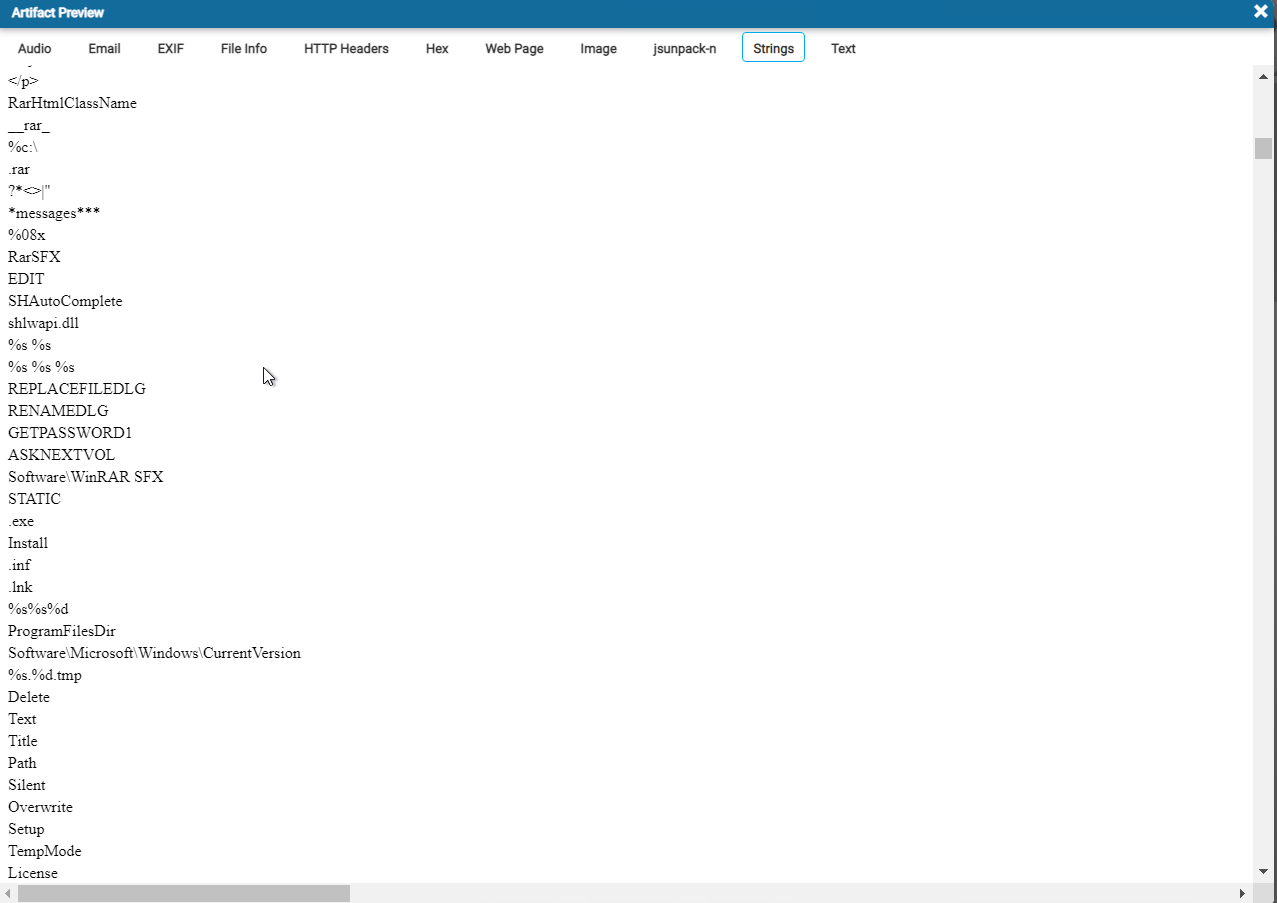
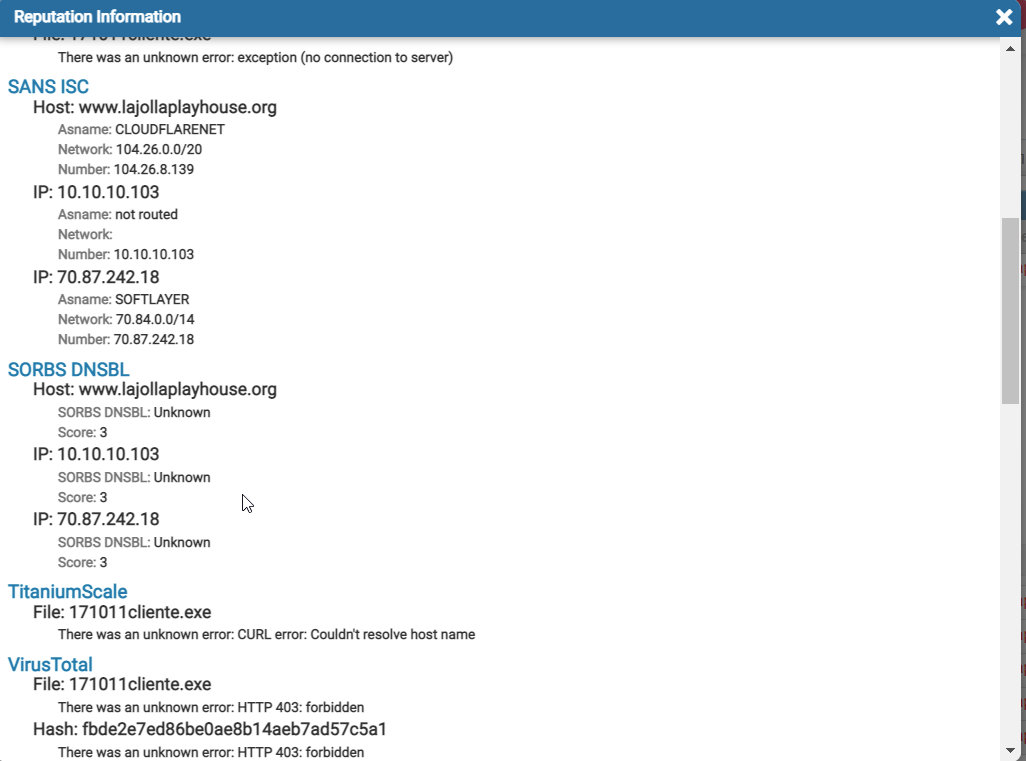
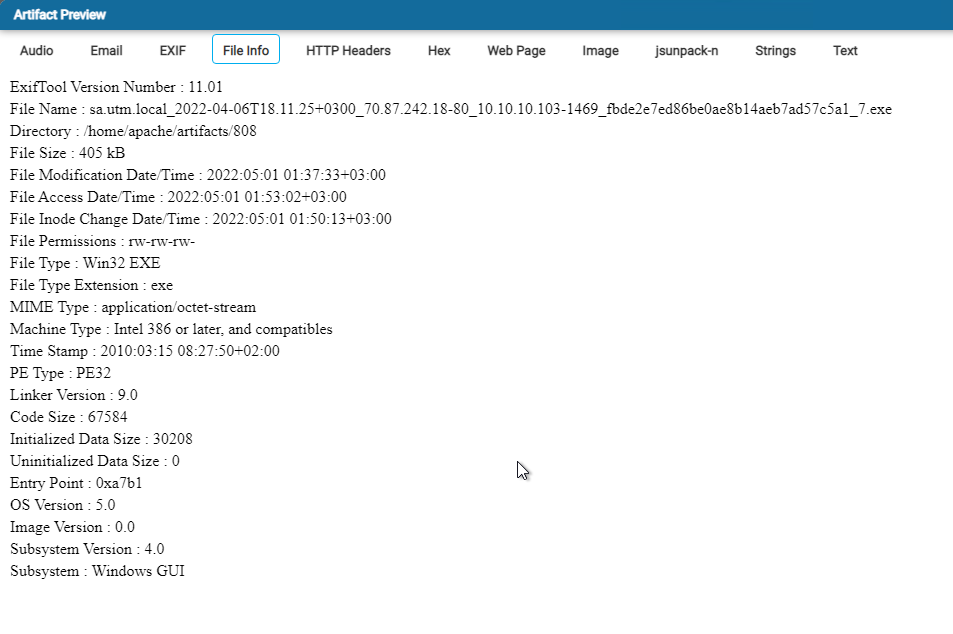
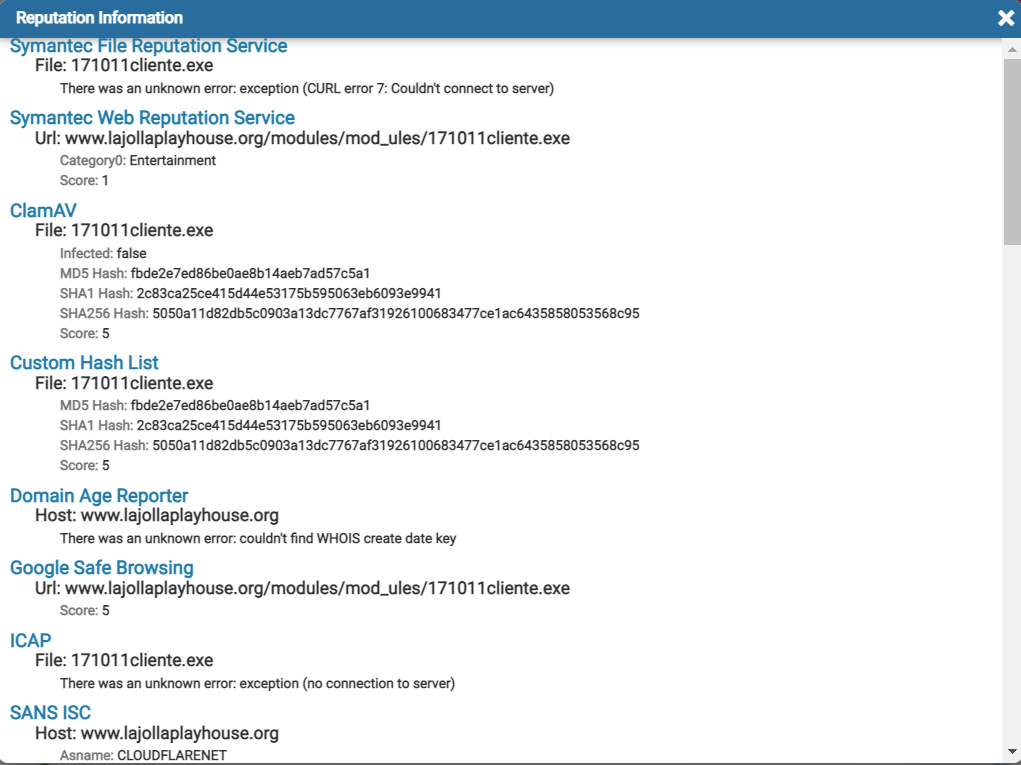
Obtineti un raport Net IPv4Initiator;



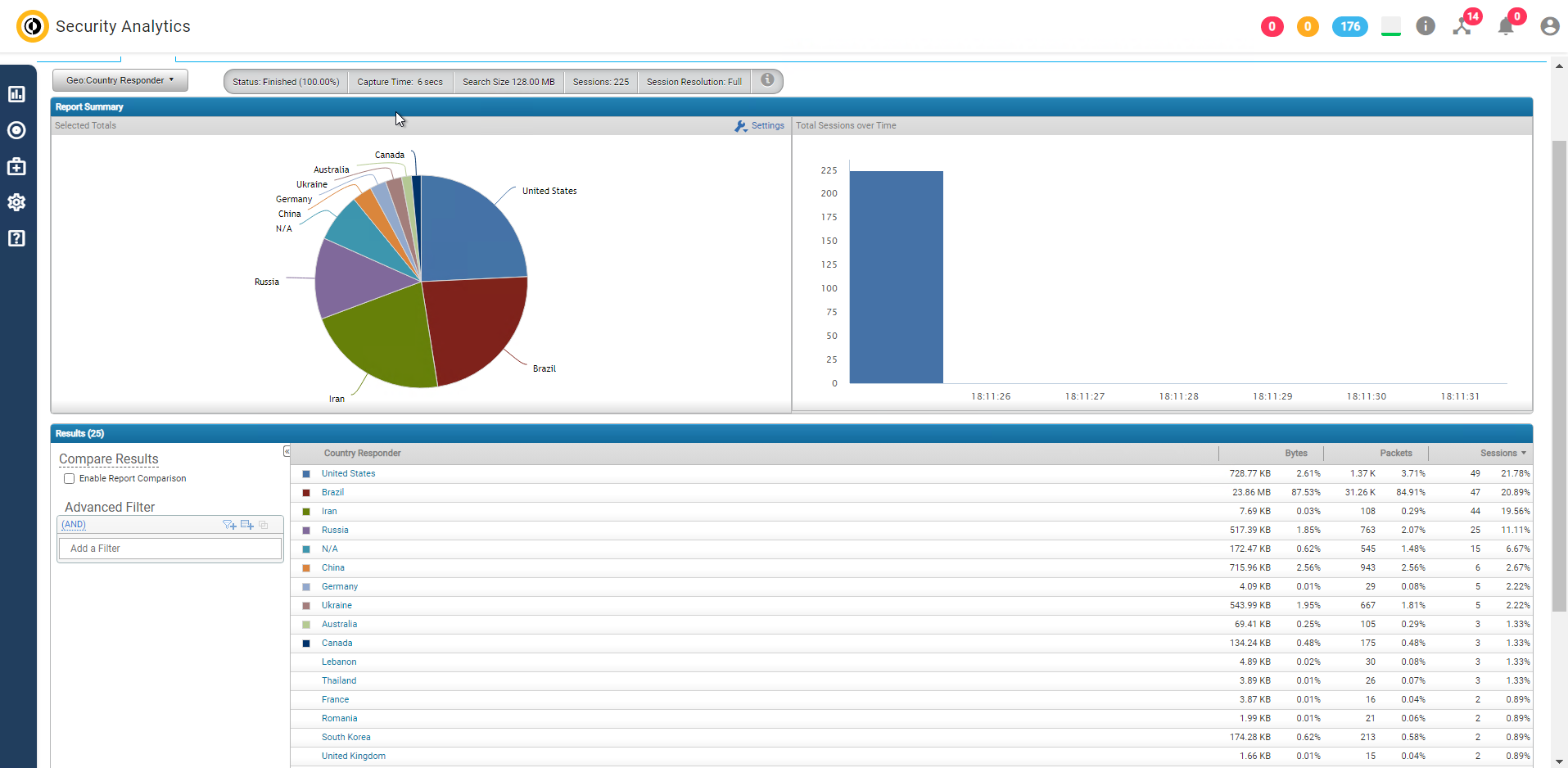
Importati Pcap-ul  malware1.pcap si sa se filtreze artefactele dupa extensia exe;



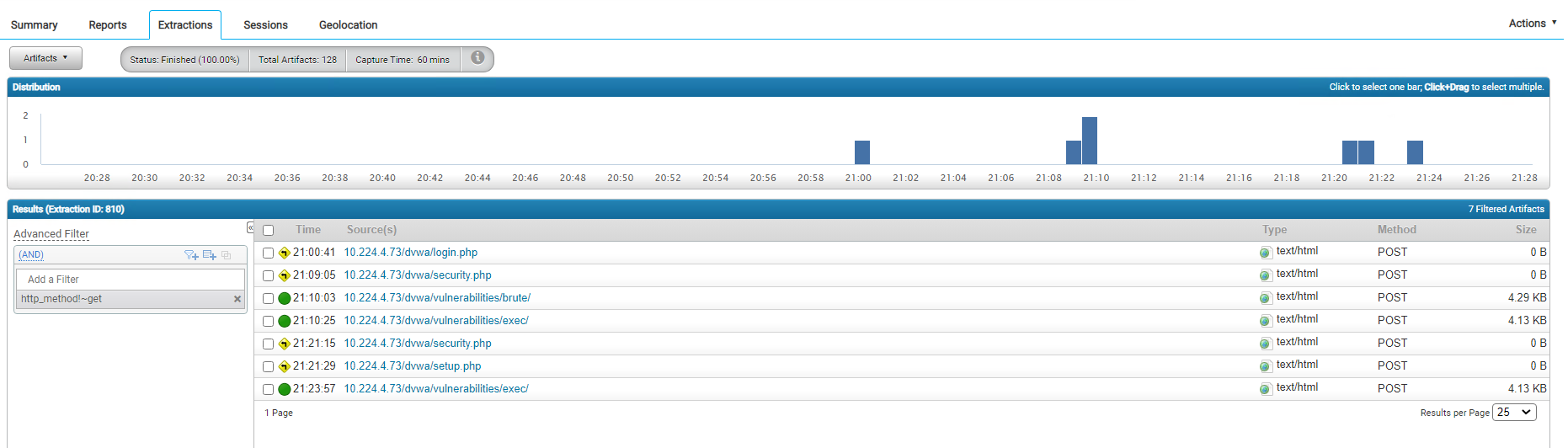
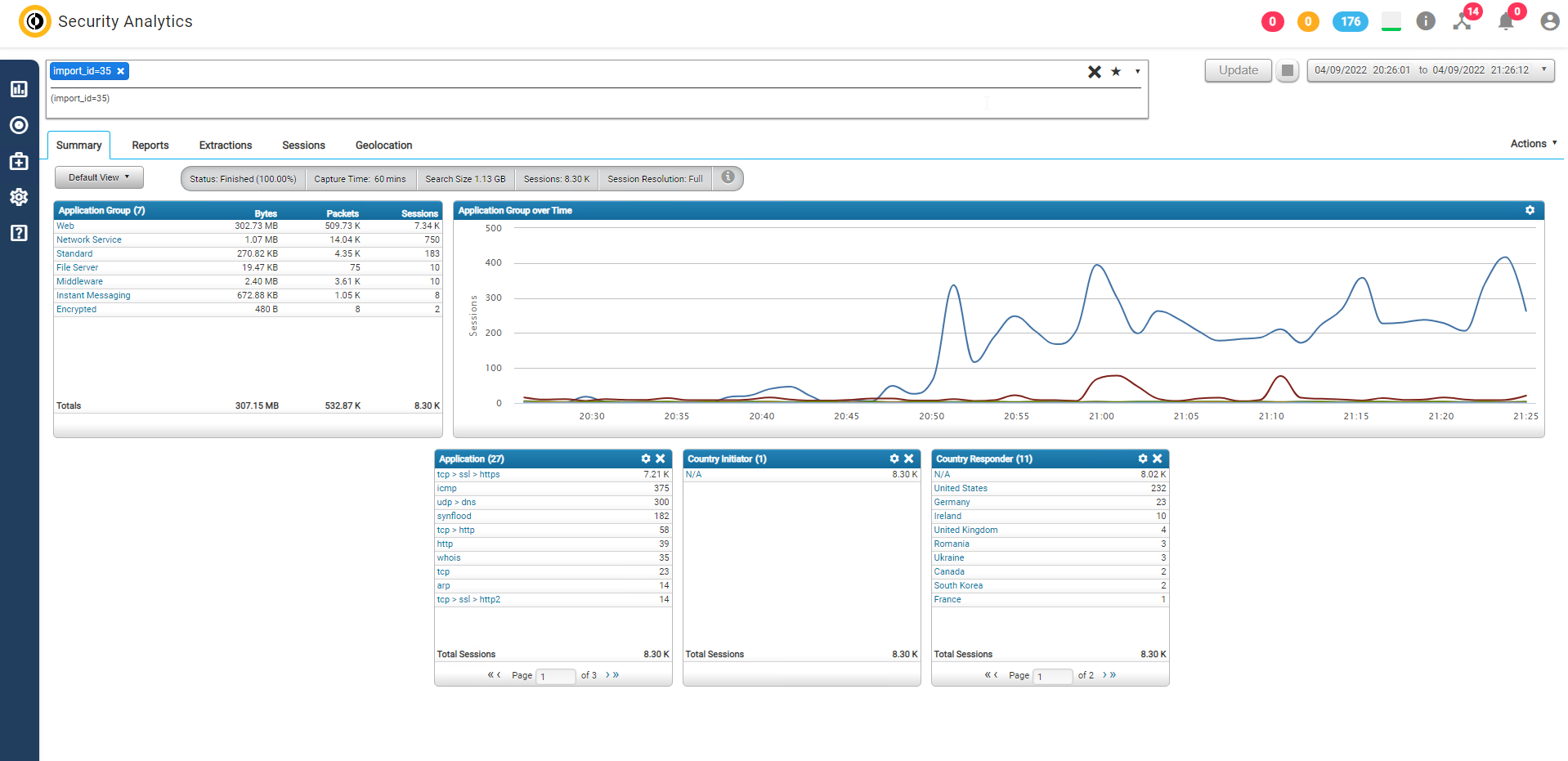
Sa se analizeze fisierele filtrate cu extensiile exe/ png inclusiv reputati acestora tinand seama si de informatiile de la <https://docs.clamav.net/> ;



Sa se realizeze un raport dupa “Geo Country Responser”.



Sa se importe Pcap-ul Set2 si sa se analizeze acesta, folosind succesiv diverse filtre (http\_method!~get; keyword="business consulting services"; keyword=mezzo\_web\_scroll\_bottom.js).



Obtineti un raport de tip🡪 

