Nagy Róbert

DARKNET

avagy az internet sötét oldala

BBS-INFO Kiadó, 2021.

A könyv nagyobb mennyiségben megrendelhető a kiadónál:
BBS-INFO Kiadó, www.bbs.hu Tel.: 407-17-07

Papírkönyv: 978-615-5477-93-5
E-book: ISBN 978-615-5477-94-2

Kiadja a BBS-INFO Kft., Budapest
Felelős kiadó: a BBS-INFO Kft. ügyvezetője
Nyomdai munkák: Biró Family Nyomda
Felelős vezető: Biró Krisztián

TARTALOMJEGYZÉK

Előszó

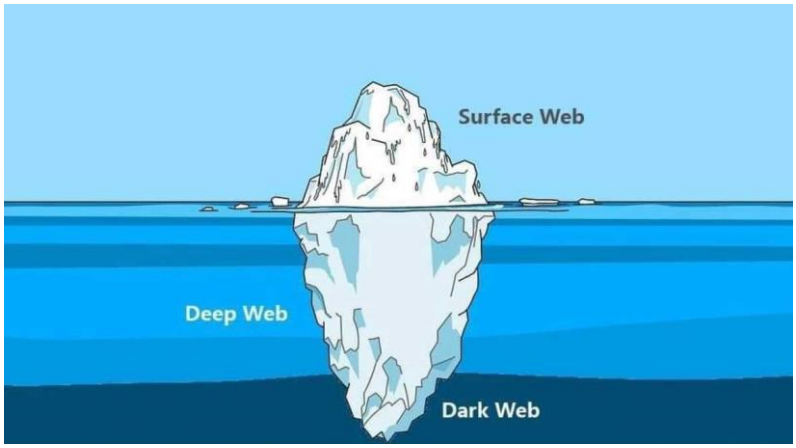
A DarkNet olyan szerverek és peer-to-peer számítógépek összessége, melyek csak speciális, titkosítást alkalmazó web böngésző segítségével érhetők el. A névtelen/anonim internetezés lehetőségét jelenti. Szélsőséges technológia, mert alkalmazható jó és rossz cél érdekében is, köztes használata viszont nem indokolt, arra a hagyományos böngészők is megfelelnek. Segítségével ki lehet játszani diktatúrákat, leleplezni a korrupciót, névtelenül megnevezni a bűnelkövetőt, ugyanakkor sajnos használható bűncselekményekkel összefüggő file-ok tárolására is. A köztudatba elsősorban a második felhasználása révén vonult be.

A könyv első felében megtanuljuk az anonim internetezést, illetve érintjük a DarkNet nemes célra történő felhasználását, melyet az alapok elsajátítása után bárki kipróbálhat saját számítógépén is. A könyv második felében a bűnügyi felhasználást vizsgáljuk azzal a céllal, hogy kielégítsük az emberek szokatlan, rendkívüli, izgalmas és titokzatos iránti vágyát, azonban arról is meggyőzzük őket, hogy saját maguk soha ne fogyasszanak online bűnügyi tartalmakat, inkább könyvből tanulják meg, milyen bűncselekmény videóknak és fájloknak ad otthont ez a világ.

A DarkNet a jelenkor egy csúcstechnológiája, melynek ismerete hozzátartozik az informatikai alapműveltséghez, azonban használata mindenkinek saját felelőssége. Lépjünk be, ha segít nekünk vagy más embernek, minden más esetben pedig kerüljük el!

1. Public Web, Deep Web, Dark Web

Az internet felépítését tartalom alapján csoportosítva jéghegy segítségével szokták ábrázolni (*1. ábra*).



1. ábra

Public Web = nyilvános Web:

A nyilvános internet a teljes világhálónak csupán 4 %-át alkotja, ez a jéghegy csúcsa, az ábrán Surface Web = felszíni háló. Olyan weboldalakat megvalósító szervereket jelent, melyek bármely számítógépről elérhetők mely rendelkezik internet hozzáféréssel és hagyományos, nyilvános webböngésző alkalmazással (a teljesség igénye nélkül pl. Mozilla, Edge, Internet Explorer, Google Chrome, Opera). A nyilvános weboldalak megjelennek keresőmotorokban is.

A keresőmotor az informatikában egy program vagy alkalmazás, amely bizonyos feltételeknek (többnyire egy szónak vagy kifejezésnek) megfelelő információkat keres valamilyen számítógépes környezetben. Az internetes keresőmotorok tipikusan két részből állnak, az egyik összegyűjti az információt, a másik pedig rendszerezi.

Deep Web = mély Web:

A Deep Web a teljes világhálónak 90 % - át alkotja, az ábrán már a víz szintje alatt található, elmerül. Olyan szerverek illetve adatbázisok összességét jelenti melyek nem jelennek meg keresőmotorokban, illetve csak beléptetési folyamat révén érhetők el, mely **felhasználónév** és **jelszó** formájában valósul meg. A Deep Web tulajdonképpen intranetek összessége.

Az intranet olyan számítógép-hálózat, amely az internetprotokollt használja, de a külvilág (az internet) felé zárt, vagy csak egy átjárón illetve tűzfalon keresztül érhető el, amely az intranet külső kapcsolatait szabályozza. Az intranet az internet mellett, de időben később megjelent fogalom. Egy belső "internet". Az interneten megszokott eszközök vállalaton, intézményen belüli használata (intra: valamin belüli). Az internet bármilyen számítógép, illetve hálózat közötti kapcsolatot lehetővé tesz, az intranet viszont sokszorosan védett belső hálózat. Míg az internetet bárki használhatja, addig az intranetet csak a belső szervezet jogosultsággal rendelkező tagjai használhatják. Tipikus intranet egy vállalat belső hálózata, amit az internettől tűzfal választ el. Az internet felől az intranet kiszolgáló berendezéseit közvetlenül nem lehet elérni, csak a tűzfalon keresztül, aminek az a feladata, hogy védelmet nyújtson a belső rendszerek és a

vállalati adatforgalom számára. Egyéb védelmi lehetőségek pl.: VPN, IP rejtő szoftver.
Példák Deep Web-re:

- Felhő alapú szolgáltatások: a felhőalapú számítástechnika (angolul „cloud computing") a számítástechnika egy ágazata. Többféle felhőalapú szolgáltatást különböztethetünk meg, a közös bennük az, hogy a szolgáltatásokat nem egy dedikált hardvereszközön üzemeltetik, hanem a szolgáltató eszközein elosztva, a szolgáltatás üzemeltetési részleteit a felhasználótól elrejtve. Ezeket a szolgáltatásokat a felhasználók hálózaton keresztül érhetik el, publikus felhő esetében az interneten keresztül, privát felhő esetében a helyi hálózaton vagy az interneten. Példa: emailezés, kép- és videómegosztó oldalak postafiókjai, közösségi média, stb. Tény, a felhő tulajdonképpen „más számítógépe".
- Multinacionális cégek, közép- és kisvállalkozások intranet hálózatai
- Kormányzati szervek, Közbiztonsági szervek, Titkosszolgálatok, Honvédség, Rendőrség intranet hálózatai
- Tudományos kutatások intranet hálózatai
- Orvosi és gyógyszerészeti kutatások intranet hálózatai

A Deep Web szerverei és adatbázisai szigorúan védettek, azonban kevésbé, mint a DarkNet infrastruktúra. Méretükből adódóan is, hiszen a teljes világháló 90%-át alkotják. Sajnos lehetséges hacker támadást indítani ellenük, tény, hogy ehhez nagyon jól és speciálisan képzett szakemberek hosszú és kitartó munkája szükséges.

Dark Web = sötét Web:

A **DarkNet** a teljes világhálónak csupán kb. 6 %-át alkotja, ez a jéghegy alja, az ábrán a legsötétebb, legsárosabb,

legmélyebb vizekig süllyed **Olyan szerverek és peer-to-peer számítógépek összességét jelenti, melyek speciális, titkosítást alkalmazó internetböngésző segítségével érhetők el.** A DarkNet a szélsőségek technológiája, mert jó és rossz célokra egyaránt használható. Segítségével ki lehet játszani diktatúrákat, leleplezni a korrupciót, ugyanakkor bűncselekményekkel összefüggő fájlok tárolására is alkalmas, a köztudatba főleg ezzel a képességével vonult be. Ezen illegális szerverek hálózatát a technika és tudomány jelenlegi állása szerint a közbiztonsági szervek nem-, vagy csak részben tudják felszámolni.

A Deep Web-hez képest erősebb a védelem, erősebb a titkosítás, illetve speciális, úgynevezett hagyma útvonalválasztást megvalósító internet böngészővel érik el az oldalakat, melyek hagyományos böngészővel nem működnek.

Bűnügyi tartalom esetében a berendezések többnyire nem hagyományos, polgári, legálisan működő internetszolgáltató épületében, szerverszobájában kapnak helyet. Az illegális szerverek speciálisan erre a célra kialakított helységekben, eldugott helyeken, minden elől rejtve találhatók. Pl. pincében, bunkerben, egy pajta alatt kialakított szobában, stb.

Végezetül egy összehasonlítás: a Deep Web-et inkább nem etikus hackerek, a DarkNet-et inkább etikus hackerek támadják. A Deep Web legális, a DarkNet bizonyos részei nem azok.

2. **Elméleti alapok, a**z internet **működése**

Az internet nem más, mint egy óriási-, a teljes földgolyót behálózó gráf.

2.1. **Gráf és hálózat elmélet**

A gráf fogalmának két alapvető meghatározása létezik:

1. A gráf pontpárok halmaza, ahol nem számít a pontok geometriai elhelyezkedése, csak az, hogy melyik pont melyik pont melyik ponttal áll összeköttetésben.

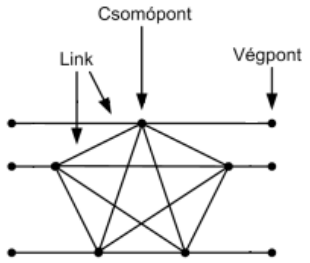
2. A síknak véges sok pontjából és az őket összekötő vonalakból álló alakzatokat gráfnak nevezzük.

A pontok a gráf pontjai (vagy csúcsai), az összekötő vonalak a gráf élei.

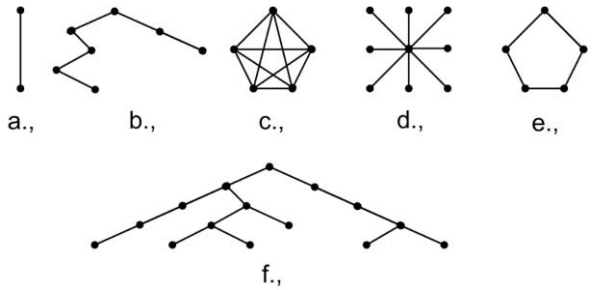
A **hálózat** szó alkalmazása inkább a gyakorlati iparágakban (pl. informatika, távközlés, közlekedés, energetika, stb.), a **gráf** szó alkalmazása inkább az elméleti matematikában terjedt el, valójában **a két dolog ugyanazt jelenti**. Hálózatok esetében a pontokat **csomópont**oknak és **végpont**oknak, az éleket **link**eknek szokás nevezni. A *2/a. ábra* a hálózatok 3 alapelemét mutatja egy egyszerűsített hálózaton:

- Végpont jelentése: a hálózat olyan pontja ahonnan csak 1 link indul ki.
- Csomópont jelentése: a hálózat olyan pontja ahonnan 2 vagy több link indul ki.

- Link jelentése: végpontot csomóponttal vagy csomópontot csomóponttal összekötő szakasz. (Megjegyzés: elméleti rajzokon a linkek lehetnek egyenes vonalak, valójában a tájon/térképen értelmezett hálózatok esetében ezek szabálytalan vonalak, mint pl. az internet esetében az UTP és optikai kábelek.)
- Fokszám jelentése: egy pontból kiinduló élek száma.



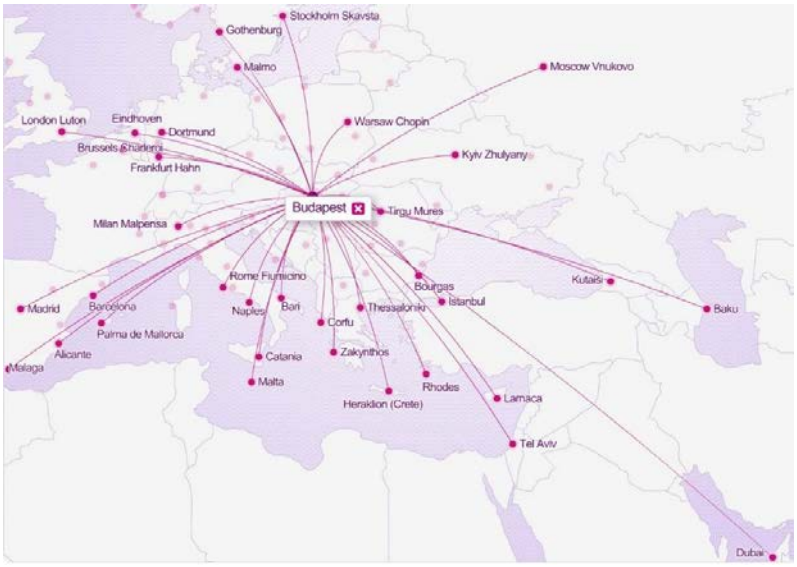
2/a. ábra



2/b. ábra

Egy valós hálózat több ezer, de akár több tízezer elemi összetevőből is állhat, a teljes internet esetében pedig ez milliárdos nagyságrendű. Egy nagy hálózat **struktúrája,** azaz **topológiája** összetett és bonyolult, de minden esetben elemi topológiákból épül fel. A *2/b. ábra* ezen elemi topológiákat ábrázolja, melyeket a fejezet további részében részletesen tárgyalunk.

- a., pont – pont topológia: 2 pont összekötésével keletkezik, a hálózat legkisebb összetevője, tulajdonképpen maga a link. Az összes többi elemi topológia és a nagy hálózat legkisebb építőeleme. Gyakorlati példák: Egy kapcsolati hálóban egy pár vagy a férj és feleség. 2 települést összekötő közútvonal. 2 vasútállomás közötti vasútvonal. Távközlésben 2 antenna közötti szabadtér.
- b., lánc topológia: 2 végpontot és minimum 1 csomópontot tartalmaz, de számos csomópontot tartalmazhat. A végpontokból mindig 1, a csomópontokból mindig 2 link indul ki. Gyakorlati példa: repülőgépek és hajók útvonala. A végpontok a repterek és kikötők, a csomópontok az útvonal fordulópontjai (ahol a jármű fordul). Megjegyezzük, hogy itt a linkek a valóságban is egyenes vonalak.
- c., szövevényes hálózati topológia (vagy más néven teljes gráf): minden pont minden ponttal összeköttetésben áll. Ebben az esetben értelemszerűen csak csomópontokról beszélhetünk, végpontokról nem. Egy n pontból álló teljes gráf minden pontjából n-1 él indul ki, példánkban a csomópontok száma n=5, az élek száma n-1=4. Gyakorlati példa: egy csoport egy közösségi oldalon ahol minden tag az összes többi tagnak ismerőse. Beszélhetünk részleges szövevényről is, ebben az esetben néhány csomópontól csak n-2, n-3, stb. él indul ki, pl.: 
- d., csillag topológia: pontosan 1 csomópontot és legalább 3 végpontot tartalmaz (emlékezzünk vissza, ha csak 2 végpont lenne, az még lánc topológia lenne). Gyakorlati példa: légitársaságok útvonalai. A *3. ábra* azt mutatja, hogy egy magyar diszkont légitársaság járataival Budapestről mely városokba lehet eljutni. Itt Budapest bázisreptérként a csillag topológia középpontja, az egyetlen csomópont, a többi város alkotja a végpontokat.

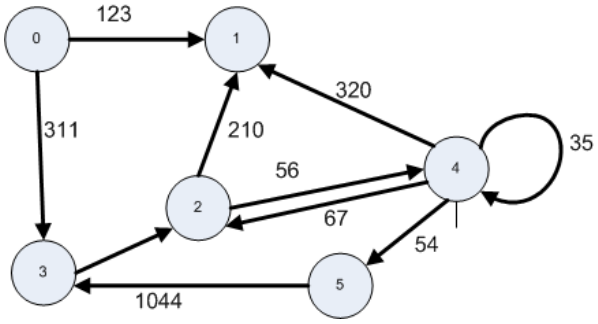


3. ábra

- e., gyűrű topológia: a lánc topológiából származtatható, de ez **zárt** lánc. Nem tartalmaz végpontokat csak csomópontokat. Minden csomópontból pontosan 2 link indul ki.
- f., fa topológia: a lánc topológiából származtatható. Olyan láncok összessége, melyeknek van közös linkjük, továbbá egy pontban futnak össze, azaz az összes lánc egyik végpontja azonos. Mindig annyi elemi láncot tartalmaznak, ahány végpontjuk van (vizsgált ábrán 6-ot). Gyakorlati példák: számítógépünk könyvtárstruktúrája, egy cég szervezeti ábrája (felsővezető – középvezetők – beosztottak).

Fejezetünk végén még az irányított gráf és súlyozott gráf fogalmakat tekintjük át. Irányított gráfról akkor beszélünk, ha az éleknek iránya is van, ezt nyíllal szokás jelölni (*4. ábra*). Súlyozott gráfban a gráf minden éléhez számértéket is

rendelünk, az él súlyát. A *4. ábrán* látható gráf súlyozott és irányított is.



4. ábra

Műsorszórás jelentése: egyirányú kép- és hangátvitel.
Távközlés jelentése: kétirányú kép, hang és adat átvitel.

Az internet távközlő hálózat - illetve országokat, kontinenseket, tengerfenekeket és az űrt behálózó távközlő hálózatok összessége - mely az előbbiek összekapcsolódásával jön létre.

Az internet illetve távközlő- és műsorszóró hálózatok vizsgálata során **a fejezetben tárgyalt gráfokat térképre kell rajzolni, illetve térképes felület felett elképzelni őket.**

- Végpont lehet pl.: számítógép, okostelefon, TV készülék, stb.. Általában a felhasználónál foglalnak helyet.
- Csomópont lehet pl.: telefonközpont, router, switch, gateway, stb. Általában a távközlési/internet/műsorszóró szolgáltató épületében foglalnak helyet.
- Három alapvető összeköttetés típus létezik: Elektromos kábel, optikai kábel, vezeték nélküli összeköttetés.

2.2. A kezdetek, és az internet ma

Az internet tervezése, fejlesztése, üzemeltetése és karbantartása szerencsére emberek sokaságának ad munkát. Évti-

zedek óta az IT és távközlési szakemberek körében, illetve a felsőoktatási intézményekben egyik legkedveltebb szakkönyv/tankönyv Andrew S. Tannenbaum – David J. Wetherall: Számítógép hálózatok című, 900 oldalas műve. Mára egyféle „Internet Bibliává" nőtte ki magát, a szerző is ebből tanult.

Idézet a Tannenbaum könyvből:

„ Az ARPANET

A történet az 1950-es évek végén kezdődik. A hidegháború tetőfokán az amerikai védelmi minisztérium (Department of Defense, DoD) egy olyan parancsnoki és irányítási hálózatot akart létrehozni, amely képes túlélni egy atomháborút. Abban az időben a teljes katonai kommunikáció a nyilvános telefonhálózatot használta, amelyet sebezhetőnek tartottak. Ennek a vélekedésnek a kiváltó oka az 1.25.(a) ábrából kiolvasható. A fekete pontok a telefonközpontokat jelölik, amelyek közül mindegyikhez több ezer telefon kapcsolódik. Ezek a központok hasonlóképpen egy magasabb szintű kapcsoló központhoz (távhívóközponthoz) kapcsolódnak. Ezzel egy olyan országos hálózat alakul ki, amely csak nagyon kevéssé redundáns („védett" a szerző megjegyzése). A rendszer sebezhetősége éppen abban rejlik, hogy elég néhány kulcsfontosságú távhívóközpontot elpusztítani ahhoz, hogy a rendszer elszigetelt részekre essen szét.

1960 körül a DoD megbízta a RAND Corporationt, hogy keressen megoldást a problémára. Az egyik munkatársuk, Paul Baran az 1.25.(b) ábrán látható, nagymértékben elosztott és hibatűrő rendszert javasolta. A központok között vezető utak hossza itt már nagyobb, mint amennyit egy analóg jel torzulás nélkül képes megtenni, ezért Baran egy digitális csomagkapcsoló megoldást javasolt bevezetni a központokban."