Hey, wie geht‘s? 😃

“Wie wär‘s mit dem Wahlpflichtfach Informatik?!“

Mag. Simon Marik

Wer bist du? 

„Bist du on-line?“

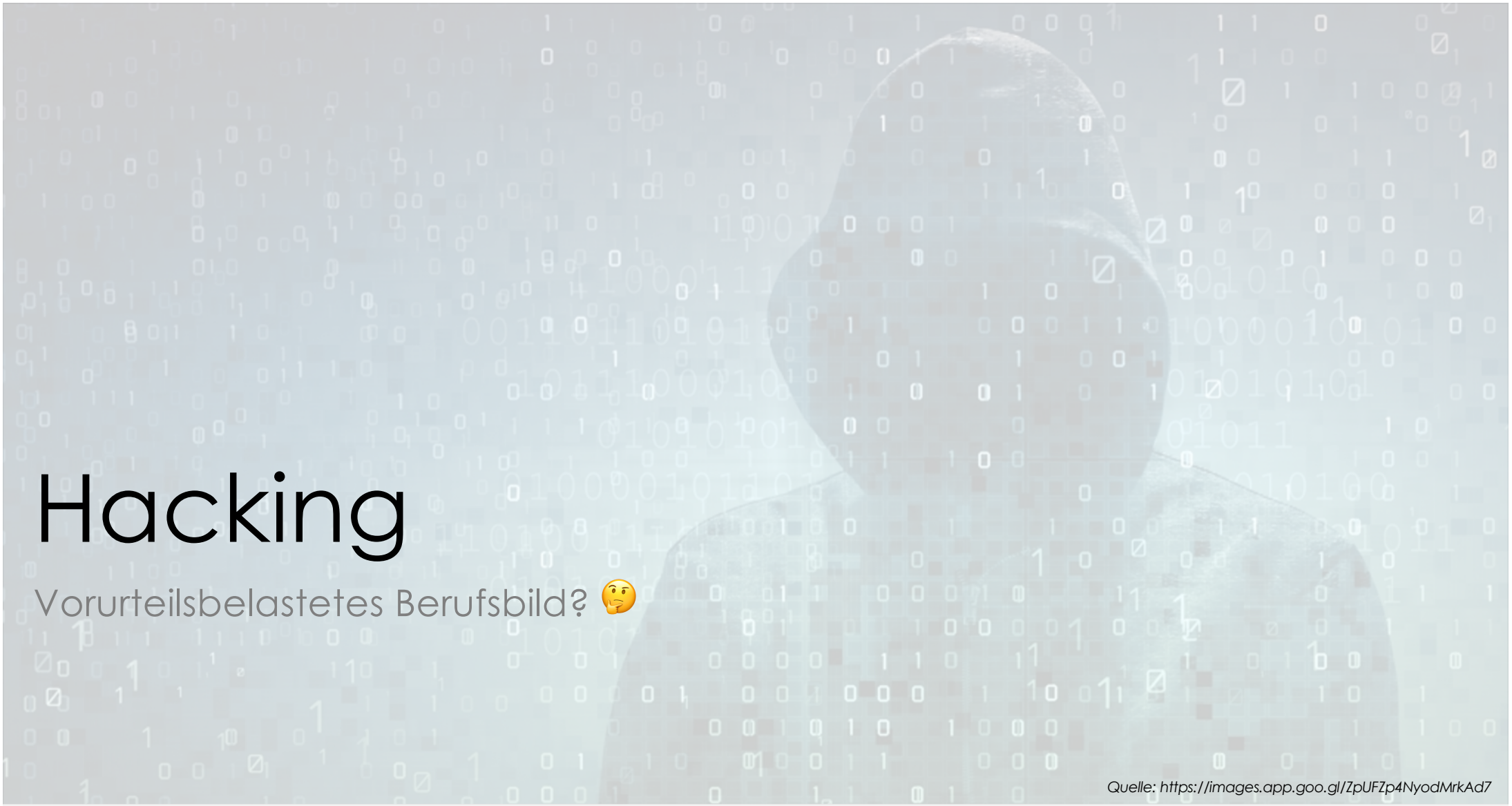
Beurteilungskriterien

MÜNDLICHE UND SCHRIFTLICHE LEISTUNGEN

- **Projekt**
  Mehrmals pro Semester
- **Interview**
  1x pro Semester
- **Beitrag**
  1x pro Schuljahr
  (Referat oder Artikel)

MITARBEIT

- **Aktive Teilnahme** am Unterrichtsgeschehen (Diskussionen, Partner- und Gruppenarbeiten usw.)
- Stundenwiederholungen, Arbeitsaufträge usw. **zeitgerecht in angemessener Qualität**
- Leistungen bei der Erarbeitung neuer Lehrstoffe **(Verständnis)**



Hacking

Vorurteilsbelastetes Berufsbild? 🤔

Quelle: https://images.app.goo.gl/ZpUFZp4NyodMrkAd7

Hacken / Hacker

- **Eine einfallsreiche Experimentierfreudigkeit…**
- Bereich Computersicherheit → Aushebelung von Sicherungsmechanismen
- Hacker beschäftigen sich mit Sicherheitsmechanismen und Schwachstellen
- Hacker-Begriff in Öffentlichkeit → Fremde d. unerlaubt in Systeme eindringen
  - Eigentlich auch Sicherheitsexperten
  - Entsprechend ist der Begriff stark positiv beziehungsweise negativgeprägt
- Hacker abgrenzbar von **Scriptkiddie**
  - Hacker besitzt tiefe Grundlagenkenntnisse, ein Scriptkiddie nicht!

Quelle: https://images.app.goo.gl/qi8maSq3osMmss9Z7

Schicke Hüte 🎩

- Unterscheidung Hacker nach Motivation und Loyalität zum Gesetz:
  - White-Hat-, Grey-Hat- und Black-Hat-Hackern
  - Black-Hats und Scriptkiddies → Cracker
- Hacken seit **1986 Strafrechtstatbestand**:
  - *„Computersabotage im Allgemeinen, und die unbefugte Manipulation von Daten im Besonderen, als spezielle Form der Sachbeschädigung – (§ 202a, § 303a und § 303b des StGB)“*
- Nach der Einführung der Gesetze zur Computerkriminalität → Abgrenzung zwischen Hackergruppen
  - Abhängig von der Gesetzmäßigkeit ihrer Tätigkeiten
- Keine klare Trennlinie zwischen **Gut** und **Böse**
  - Wenig Bezug auf real existierende Personen
  - Eher Begrifflichkeiten für eine bestimmte Art des Hackens

White-Hats

- Verwendung des Wissens:
  - Innerhalb der Gesetze
  - Innerhalb der **Hackerethik**
- Die ethischen Grundsätze des Hackens:
  - Zugang zu Computern soll frei sein
  - Alle Informationen müssen frei sein
  - Misstraute Autoritäten → fördert Dezentralisierung
  - Beurteile einen Hacker nach dem, was er macht
    - nicht nach üblichen Kriterien (Aussehen, Alter usw.)
  - Computer können Kunst und Schönheit schaffen
  - Computer können Leben zum Besseren verändern
  - Stöbere nicht in den Daten anderer Leute
  - Öffentliche Daten nützen, private Daten schützen
- Arbeitsbereich:
  - Ausführung eines professionellen Penetrationstests
  - Aufdeckung von Sicherheitslücken in Unternehmen

Quelle: https://images.app.goo.gl/EwinBrde1YFpu1Un7

Grey-Hats

- Verwendung des Wissens:
  - Verstoßen möglicherweise gegen Gesetze
  - Restriktive Auslegung der Hackerethik
- Erreichung eines **höheren Ziels** im Vordergrund
- Arbeitsbereich:
  - Veröffentlichung von Sicherheitslücken
    - Macht Leugnen unmöglich
    - Zwingt die Verantwortlichen dazu, diese zu beheben
- Grey-Hats sind nicht eindeutig als **Gut** oder **Böse** einzustufen!

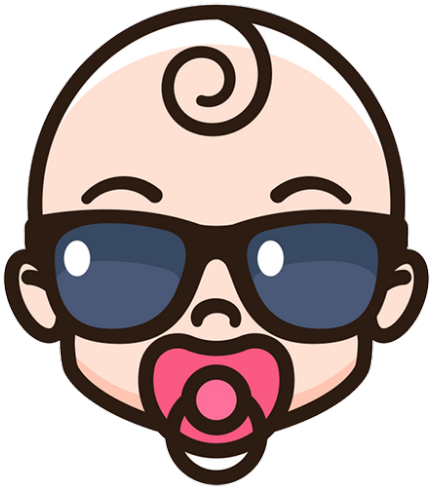
Quelle: https://images.app.goo.gl/EwinBrde1YFpu1Un7

Black-Hats

- Verwendung des Wissens:
  - Handeln mit krimineller Energie
  - Im Auftrag von Regierungen oder Organisationen
  - Beabsichtigen Zielsysteme zu beschädigen oder Daten zu stehlen
    - Sogenannter **„Cyberkrieg“**
- Arbeitsbreich:
  - Widerrechtlichen Manipulation von Software
  - Teil der illegalen **Warez-Szene**
    - Abgrenzung zur legalen **Cracker-Szene** begeisterter Programmierer
    - Grenzen sind hier fließend!

Quelle: https://images.app.goo.gl/EwinBrde1YFpu1Un7

Cracker



Quelle: https://images.app.goo.gl/mbEwJ7wzuAFnisuv8

- Definition Cracker nach **Jargon File (Kompendium) 1990**:
  - Hacker, die ihre Aktivitäten auf die Umgehung von Sicherheitsmechanismen legen → **Cracker**
  - Definition von der Presse nicht wahrgenommen oder weitestgehend ignoriert
- Hacker aus dem Sicherheitsbereich (gesetzestreuer Teil):
  - Mitverwendungsanspruch des Hackerbegriffs
  - Keine Akzeptanz der Bezeichnung als Cracker (dunkel gefärbte Richtung)
- **Scriptkiddies** zählen innerhalb der Computersicherheit zu den Crackern!
  - Nutzen vorgefertigte Automatismen (mit Anleitung), um in fremde Computersysteme einzudringen oder sonstigen Schaden anzurichten
  - Obwohl notwendige Grundlagenkenntnis fehlt → Öffentlichkeitsbegriff dennoch **Hacker**

Techniken I

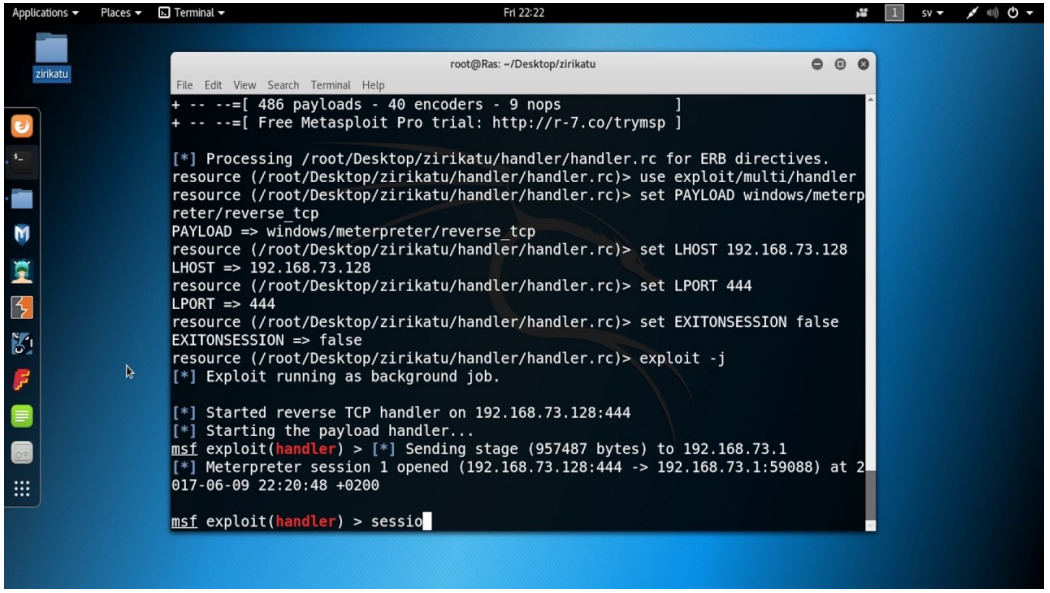
- **Virus / Würmer**
- **Social Engineering**
  - Gesellschaftliche Kontakte bringen begehrten Informationen
- **Trojanisches Pferd**
  - Als nützliche Anwendung getarnt → Erfüllt im Hintergrund, ohne Wissen des Anwenders, eine andere Funktion
- **Backdoor**
  - Ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer
    - Über Universalpasswort des BIOS
    - Über spezielle Software (Trojaner), die Fernzugriff auf das Computersystem ermöglicht
- **Rootkits**
  - Objekte und Aktivitäten vor den Augen des Anwenders verbergen
  - Installation am kompromittierten System nach Einbruch in das Computersystem
  - Führt geheime Prozesse aus und versteckt Dateien

Techniken II

- **Denial of Service (DoS)**
  - Außerstandsetzung eines Netzwerkdienstes → z.B. durch Überlastung
- **Exploit**
  - Nutzt spezifische Schwächen oder Fehlfunktionen eines anderen Computerprogramms aus
    - Erlangung erweiterter Privilegien
    - Ausführung einer DoS-Attacke
- **Vulnerability Scanner**
  - Automatische Analyse von Computersystemen
  - Hilfsprogramme suchen nach Sicherheitslücken in Anwendung, Computer oder Netzwerk
  - Helfen Anfälligkeiten zu erkennen
- **Sniffer**
  - Realisiert Datenverkehr eines Netzwerks oder eines angeschlossenen Gerätes
    - Empfang, Aufzeichnung, Darstellung und Auswertung von Daten
- **Keylogger**
  - Technik zum Aufzeichnen der Tastatureingaben

Voraussetzungen 🤓

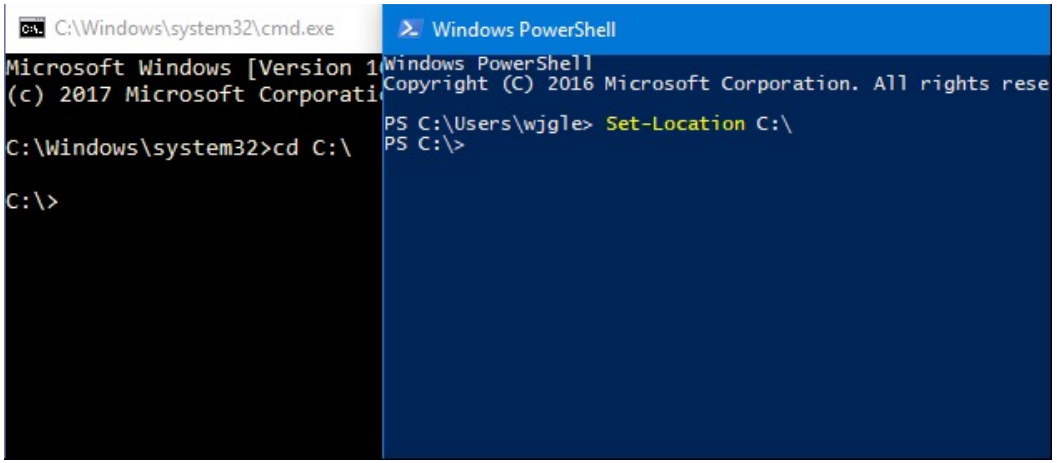
- Grundkenntnisse in Programmiersprachen
  - PHP
  - JavaScript
  - SQL
  - Skriptsprachen
- Vertiefende Betriebssystemkenntnisse
  - Linux, Windows, Virtualisierung
- Kenntnisse in der Netzwerktechnik
  - Komplexe Netzwerksysteme
  - Tor-Netzwerke
- Hardware
  - Physisch (Firewall, Fortigate usw.)
  - Virtuell (Proxy usw.)



Quelle: https://images.app.goo.gl/22dsWsc31YUy6kK36

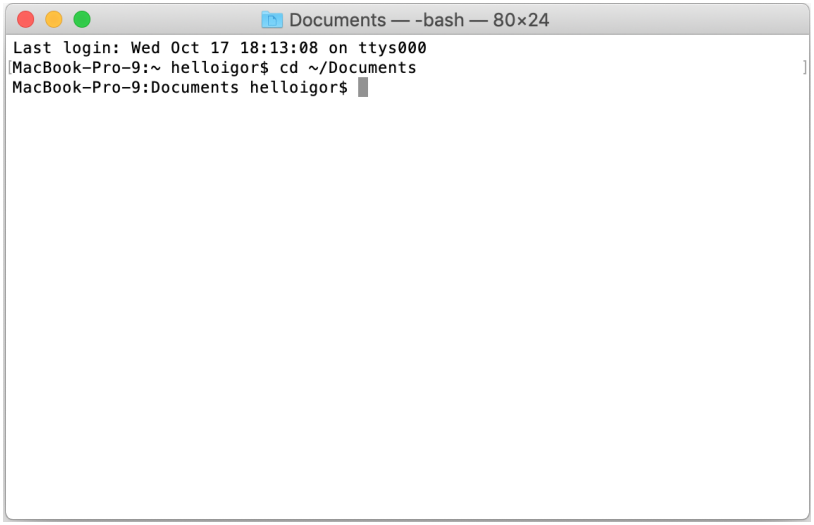
Shells

CMD & PowerShell – WINDOWS



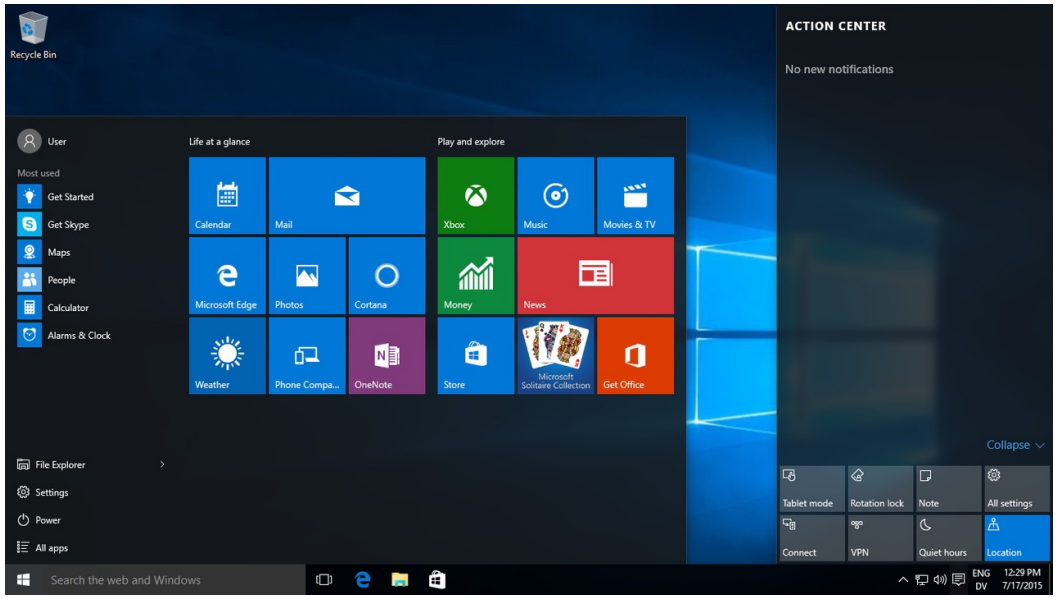
Quelle: https://images.app.goo.gl/9UX3DoP4kRqeXqCC7

Terminal – macOS / Linux

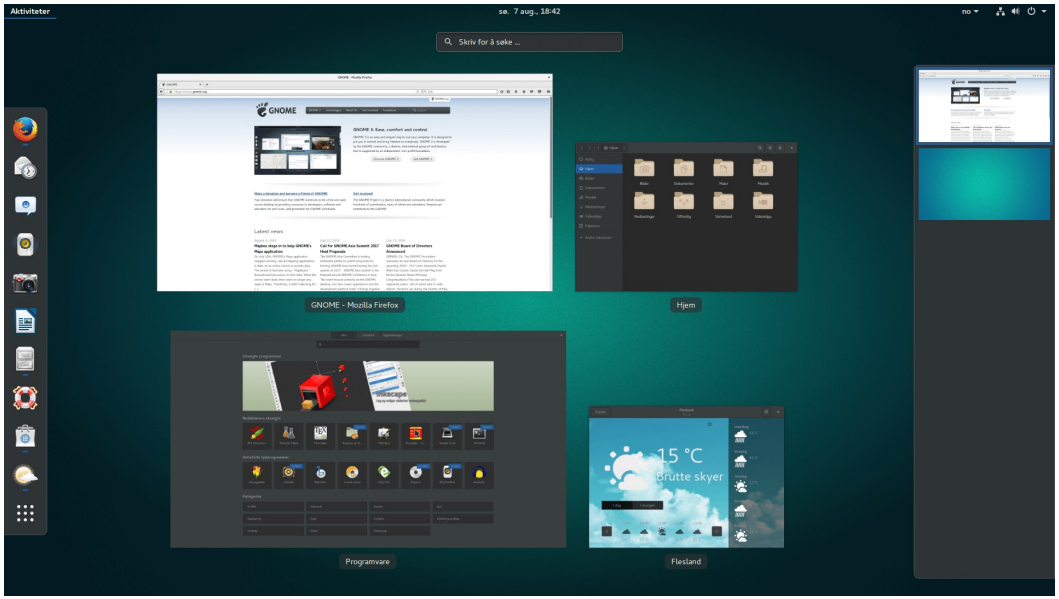


Quelle: https://images.app.goo.gl/baG24L6kJKtyctcd9

Alternative: GUI – Graphical User Interface

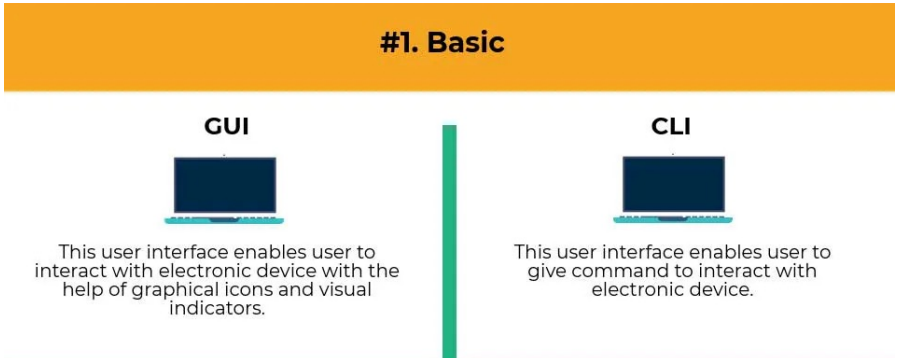


Quelle: https://images.app.goo.gl/f8vRHsUQveZq6RPw8

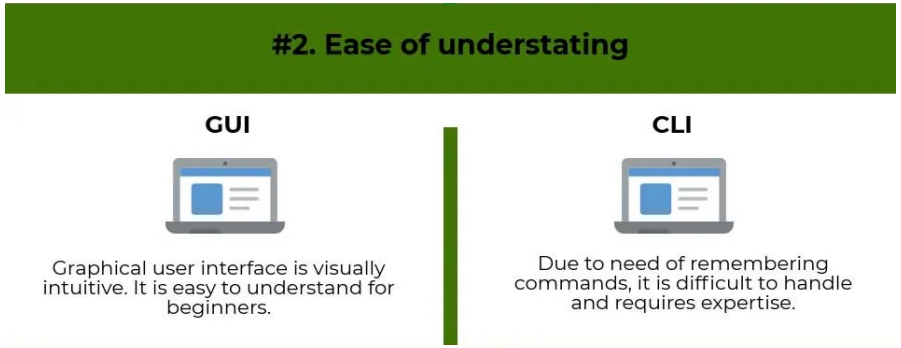


Quelle: https://images.app.goo.gl/X9QxHT2q2ftr3qsYA

GUI vs. CLI (Command Line Interface)

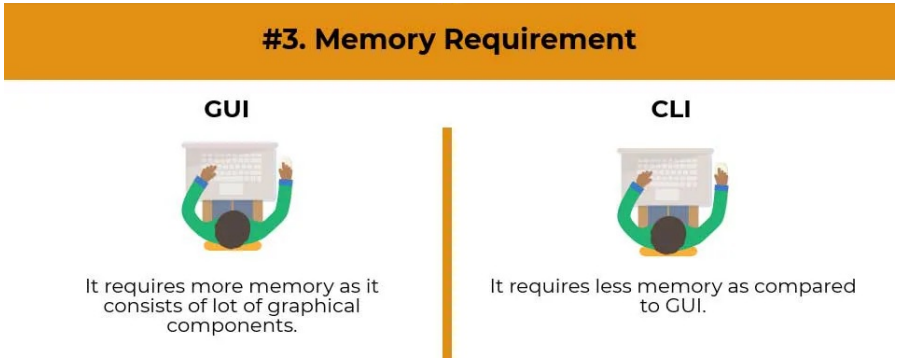


Quelle: https://images.app.goo.gl/5p3hrgynjdwrexXf8

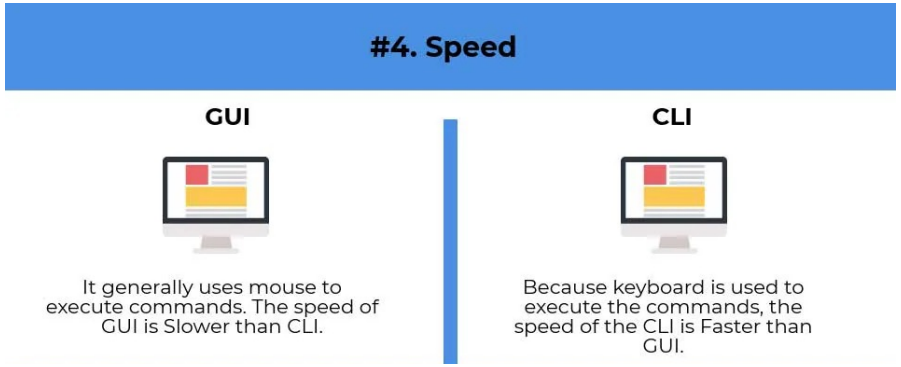


Quelle: https://images.app.goo.gl/5p3hrgynjdwrexXf8

GUI vs. CLI (Command Line Interface)

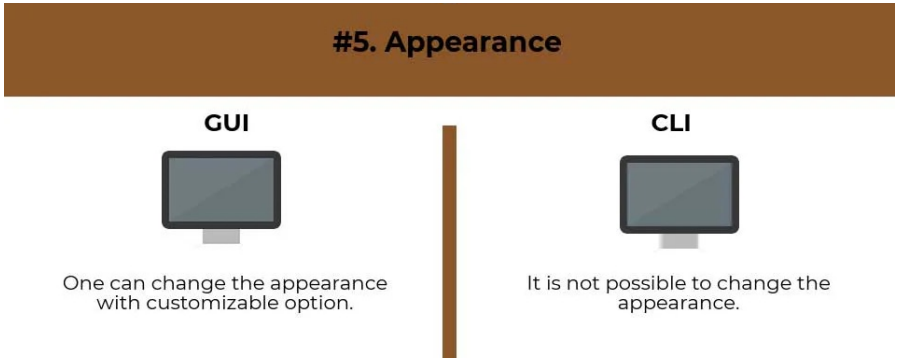


Quelle: https://images.app.goo.gl/5p3hrgynjdwrexXf8



Quelle: https://images.app.goo.gl/5p3hrgynjdwrexXf8

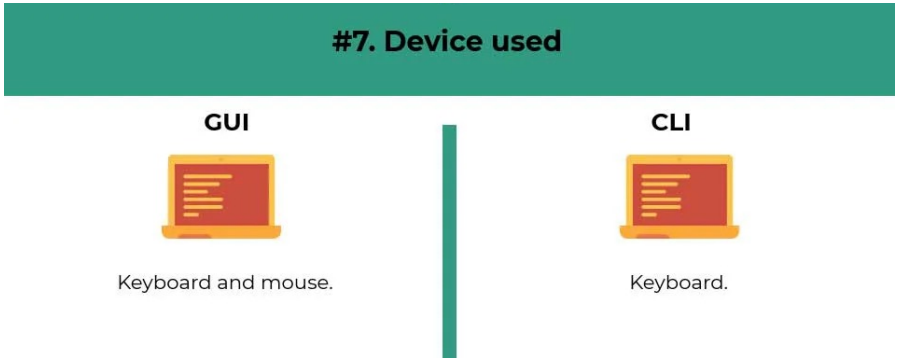
GUI vs. CLI (Command Line Interface)



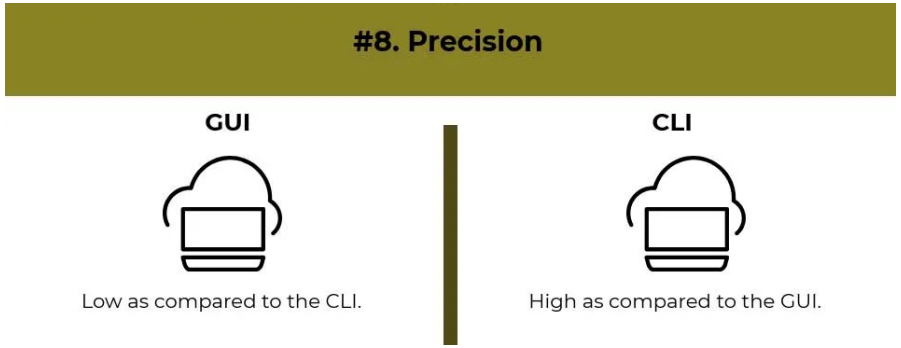
Quelle: https://images.app.goo.gl/5p3hrgynjdwrexXf8

Quelle: https://images.app.goo.gl/5p3hrgynjdwrexXf8

GUI vs. CLI (Command Line Interface)



Quelle: https://images.app.goo.gl/5p3hrgynjdwrexXf8



Quelle: https://images.app.goo.gl/5p3hrgynjdwrexXf8