Here’s your sentence-by-sentence breakdown in professional study note format — all critical details included, fully expanded for comprehension, and formatted so you can paste directly into Word without extra spacing issues.

**Web Browser Installation – Detailed Study Notes**

1. **Lesson Overview**
   * Topic: How to install a web browser from trusted sources.
   * Emphasis: Always choose reputable, verifiable download locations.
2. **Definition of Trusted Sources**
   * A trusted source is a reputable vendor or platform where software integrity is verified.
   * Examples: Microsoft Store, Apple App Store, or official vendor websites.
3. **Microsoft Store as a Trusted Source**
   * Applications downloaded from the Microsoft Store are digitally signed by the vendor.
   * Digital signatures prove authenticity and confirm the file is unaltered.
4. **Limitation of App Stores**
   * Not all browsers are available in the Microsoft Store.
   * Example: Firefox and Chrome must be downloaded from their official websites.
5. **Direct Website Downloads**
   * Google Chrome: google.com/chrome/downloads
   * Firefox: mozilla.org/en-US/firefox/new/
   * Opera: Available both in Microsoft Store and via direct download.
6. **Installation via Microsoft Store**
   * Steps:
     1. Select browser in the store.
     2. Click **Install**.
     3. Store verifies file hash against a known good value.
     4. Matching hash confirms file integrity.
     5. Browser installs automatically and appears in the Start Menu.
7. **Installation via Direct Download**
   * Steps:
     1. Visit official vendor website.
     2. Click download link (e.g., Firefox).
     3. File saves to Downloads folder.
     4. Run installer and follow setup wizard.
     5. Administrator privileges may be required.
     6. Installation completes and browser launches.
8. **File Integrity Verification (Hash Checking)**
   * Purpose: Ensure file has not been modified since it was released by the vendor.
   * Hash value = digital fingerprint of a file (e.g., SHA256).
   * Even a 1-bit change results in a completely different hash.
   * if a file’s calculated hash does **not** match the vendor-provided hash, that means the file has been altered in some way since it was originally released.
9. **Hash Verification Process in Windows**
   * Utility: certutil (built into Windows).
   * Command:
   * certutil -hashfile <filename> sha256
   * Compare generated hash with the vendor-provided hash.
   * Exact match confirms file authenticity.
10. **Example – Kali Linux Download Verification**
    * Vendor provides SHA256 hash before download.
    * After download, run certutil to compute hash.
    * Verify that beginning and ending characters match vendor hash.
    * Matching all characters ensures the file is trusted.
11. **Importance of Trusted Sources**
    * Untrusted sources may embed malware, adware, or Trojans into legitimate software.
    * Malicious installers can appear identical to official software.
    * Risks: Data theft, unauthorized access, system compromise.
12. **High Sensitivity of Web Browsers**
    * Browsers handle confidential data:
      1. Banking credentials
      2. Personal information
      3. Health records
    * A compromised browser can lead to severe privacy breaches.
13. **Best Practices for Browser Installation**
    * Use official app stores (Microsoft Store, Apple App Store).
    * If unavailable, use the official browser website.
    * Verify downloads using hash values when possible.